McAfee
An Intel Company

Installationshandbuch
Revision A

McAfee Web Gateway 7.4.2

COPYRIGHT
Copyright © 2014 McAfee, Inc. Keine Vervielfältigung ohne vorherige Zustimmung.

MARKEN
McAfee, das McAfee-Logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure sind Marken oder eingetragene Marken von McAfee, Inc. oder der Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

Produktnamen, Funktionsbezeichnungen und Beschreibungen können jederzeit unangekündigt geändert werden. Die jeweils aktuellen Informationen zu Produkten und Funktionen finden Sie unter mcafee.com.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung
HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Vorwort **5**
Informationen zu diesem Handbuch . . . 5
Zielgruppe . . . 5
Konventionen . . . 5
Quellen für Produktinformationen . . . 6

1 Einführung **7**
Hauptfunktionen von Web Gateway . . . 7
Einrichtungsabläufe für Web Gateway . . . 8

2 Einrichtung von Web Gateway **9**
Allgemeine Schritte zum Einrichten von Web Gateway . . . 9
Überprüfen der Anforderungen . . . 10
Überprüfen der standardmäßigen Erstkonfigurationseinstellungen . . . 11
Einrichten einer physischen Appliance mit vorinstallierter Software . . . 12
Einrichten einer physischen Appliance mit heruntergeladener Software . . . 12
Herunterladen der Software für eine physische Appliance . . . 13
Installieren der heruntergeladenen Software auf einer physischen Appliance . . . 13
Einrichten einer virtuellen Appliance . . . 14
Herunterladen der Software für eine virtuelle Appliance . . . 14
Installieren der heruntergeladenen Software auf einer virtuellen Appliance . . . 15
Einstellungen für virtuelle Maschinen . . . 15
Implementieren der Erstkonfigurationseinstellungen . . . 16
Implementieren der standardmäßigen Erstkonfigurationseinstellungen . . . 16
Implementieren eigener Einstellungen für die Erstkonfiguration . . . 17
Anmelden bei der Benutzeroberfläche . . . 18
Arbeiten mit dem Einrichtungs-Assistenten . . . 18
Aktivieren des Produkts . . . 18
Konfigurieren weiterer Ersteinstellungen . . . 20
Beheben von Problemen durch Herstellen einer Verbindung mit den Download-Servern . . . 21
Aktivieren von Web Gateway mit einem temporären Lizenzschlüssel . . . 22
Aufspielen eines neuen Images auf eine Appliance . . . 22
Standardeinstellungen für eine serielle Systemkonsole . . . 23
Anschlusszuweisungen auf einer physischen Appliance . . . 23

3 Installieren einer PCI-Karte **29**
Unterstützte HSM-Karten . . . 29
Unterstützte Glasfaser-Netzwerkschnittstellenkarten . . . 29
1GbE-Glasfaser-Netzwerkschnittstellenkarte . . . 30
10GbE-Glasfaser-Netzwerkschnittstellenkarte . . . 32
Installieren einer PCI-Karte . . . 34

4 Installation der Hardware-Verwaltungs-Tools **37**
Tools für die Verwaltung der Web Gateway-Hardware . . . 37
Installieren des Plattformvertraulichkeitstest-Tools . . . 38

Ausführen eines Hardwaretests mit dem Plattformvertraulichkeitstest-Tool 39
Konfigurieren des Remote Management Module 39
Installieren der Active System Console 40
Aktivieren des SNMP-Subagenten 41

5 Installation von Web Gateway auf einem Blade-Server 43
Unterstützte Blade-Server und Gehäuse 43
Installation des Blade-Server-Systems 43
Vorbereiten der Installation des Blade-Server-Systems 44
Installieren des Blade-Server-Systems 44
Netzwerkeinrichtung von Web Gateway auf einem Blade-Server 49
Proxy-Hochverfügbarkeit auf einem Blade-Server 50
Proxy mit externem Lastausgleich auf einem Blade-Server 51
Transparente Modi auf einem Blade-Server 52
Anschlusszuweisungen auf einem Blade-Server 53

Index 57

Vorwort

In diesem Installationshandbuch werden die Abläufe zur Einrichtung von McAfee® Web Gateway, Version 7.4.2, sowie verschiedener weiterer Geräte erläutert, die mit dem Produkt ausgeführt werden können.

Inhalt

- *Informationen zu diesem Handbuch*
- *Quellen für Produktinformationen*

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die vorliegende McAfee Dokumentation wurde sorgfältig recherchiert und für eine bestimmte Zielgruppe verfasst.

Die Informationen im vorliegenden Handbuch richten sich vornehmlich an folgende Zielgruppe:

- **Administratoren**: Personen, die das Sicherheitsprogramm des Unternehmens implenentieren und durchsetzen

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.
Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	Hinweis: Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	Tipp: Vorschläge und Empfehlungen.

Wichtig/Vorsicht: Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.

Warnung: Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Quellen für Produktinformationen

Nach der Veröffentlichung eines Produkts werden Informationen zu dem Produkt im Online-Knowledge Center von McAfee eingegeben.

Vorgehensweise

1 Rufen Sie das McAfee ServicePortal unter http://support.mcafee.com auf, und klicken Sie auf **Knowledge Center**.

2 Geben Sie einen Produktnamen ein, wählen Sie eine Version, und klicken Sie dann auf **Suchen**, um eine Liste der Dokumente anzuzeigen.

1 Einführung

McAfee® Web Gateway (Web Gateway) ist ein Web-Sicherheitsprodukt, das Ihr Netzwerk vor Bedrohungen aus dem Web schützt, unter anderem vor Viren und sonstiger Malware, unangemessenen Inhalten, Datenlecks und ähnlichen Problemen. Zudem werden die Einhaltung gesetzlicher Bestimmungen (Compliance) und eine produktive Arbeitsumgebung sichergestellt.

Web Gateway wird als Appliance ausgeführt, die Ihr Netzwerk mit dem Web verbindet und dabei den aus- und eingehenden Datenverkehr filtert. Bösartige und unangemessene Inhalte werden blockiert, während nützlicher Datenverkehr passieren darf.

Der Filterprozess wird durch Web-Sicherheitsregeln gesteuert, die Sie sehr flexibel konfigurieren und somit auf die Anforderungen Ihres Netzwerks zuschneiden können.

Inhalt

- *Hauptfunktionen von Web Gateway*
- *Einrichtungsabläufe für Web Gateway*

Hauptfunktionen von Web Gateway

Das Filtern von Web-Datenverkehr ist ein komplexer Prozess. Die Hauptfunktionen von Web Gateway tragen auf unterschiedliche Weise zu diesem Prozess bei.

- **Abfangen und Übertragen von Web-Datenverkehr**: Die Proxy-Funktionen einer Web Gateway-Appliance fangen Anfragen ab, die von Benutzern Ihres Netzwerks an das Internet gesendet werden. Diese werden entsprechend den Ergebnissen der Filterung an ihr jeweiliges Ziel übertragen. Von den Zielen an das Netzwerk gesendete Antworten werden ebenso abgefangen und gefiltert.
- **Authentifizieren von Benutzern**: Die Authentifizierungsfunktionen filtern die Benutzer Ihres Netzwerks, wobei unterschiedliche Authentifizierungsmethoden zur Anwendung kommen. Damit können Sie steuern, welchen Personen aus dem Inneren des Netzwerks der Zugriff auf das Internet gestattet wird.
- **Filtern von Web-Objekten**: Die Web-Filterfunktionen filtern Objekte, wobei verschiedene Arten der Filterung angewendet werden, z. B. Filterung auf Viren und Malware, URL-Filterung, Medientypfilterung und Anwendungsfilterung, um alle Bedrohungen aus dem Internet abzudecken.
- **Überwachen des Filterprozesses**: Ein umfassender Überblick über den Filterprozess wird durch die Überwachungsfunktionen geliefert. Hierzu zählen ein Dashboard für Warnungen und Statusinformationen sowie Funktionen für Protokollierung, Verfolgung und Fehlerbehebung.

Einrichtungsabläufe für Web Gateway

Die Vorgänge zum Einrichten einer Web Gateway-Appliance variieren je nach Plattform, auf der Web Gateway ausgeführt werden soll und je nach Vorgehensweise beim Abrufen und Installieren der Appliance-Software auf der Plattform.

Sie können Web Gateway wie folgt einrichten:

- **Physische Appliance**

  Beim Ausführen von Web Gateway als physische Appliance erfolgt die Einrichtung auf einer Hardware-Plattform. Die Appliance-Software wird wie folgt verfügbar gemacht:

  - **Vorinstallierte Software**: Wenn Sie eine neue Hardware-Plattform für Web Gateway erwerben, ist die Appliance-Software darauf bereits vorinstalliert.
  - **Heruntergeladene Software**: Wenn Sie die vorinstallierte Software nicht verwenden möchten, können Sie die Software auch über das McAfee Content & Cloud Security Portal im ISO- oder USB-Format herunterladen und installieren.

- **Virtuelle Appliance**

  Wenn Sie Web Gateway als virtuelle Appliance ausführen, richten Sie Web Gateway auf einer virtuellen Maschine ein, die Sie in einem geeigneten Host-System erstellen.

  Sie können die Appliance-Software im ISO-Format über das McAfee Content & Cloud Security Portal herunterladen und installieren.

2 Einrichtung von Web Gateway

Zum Einrichten von Web Gateway müssen Sie eine Reihe von Aktivitäten ausführen, z. B. Ihre Installationsmaterialien überprüfen, die Ersteinstellungen konfigurieren und sich bei der Benutzeroberfläche anmelden.

Der Einrichtungsablauf variiert je nach Plattform, auf der die Appliance-Software installiert wird sowie je nach Bereitstellungsart der Software.

Wenn Sie sich nach Abschluss der Installation erstmalig bei der Benutzeroberfläche anmelden, müssen Sie außerdem eine Lizenz importieren und das Produkt aktivieren.

Inhalt

- *Allgemeine Schritte zum Einrichten von Web Gateway*
- *Überprüfen der Anforderungen*
- *Überprüfen der standardmäßigen Erstkonfigurationseinstellungen*
- *Einrichten einer physischen Appliance mit vorinstallierter Software*
- *Einrichten einer physischen Appliance mit heruntergeladener Software*
- *Einrichten einer virtuellen Appliance*
- *Implementieren der Erstkonfigurationseinstellungen*
- *Anmelden bei der Benutzeroberfläche*
- *Arbeiten mit dem Einrichtungs-Assistenten*
- *Aktivieren von Web Gateway mit einem temporären Lizenzschlüssel*
- *Aufspielen eines neuen Images auf eine Appliance*
- *Standardeinstellungen für eine serielle Systemkonsole*
- *Anschlusszuweisungen auf einer physischen Appliance*

Allgemeine Schritte zum Einrichten von Web Gateway

Führen Sie die folgenden allgemeinen Schritte aus, um eine Web Gateway-Appliance einzurichten.

Vorgehensweise

1 Überprüfen Sie, ob die Voraussetzungen für die Einrichtung erfüllt sind.

2 Überprüfen Sie die standardmäßigen Erstkonfigurationseinstellungen.

3 Installieren Sie die Appliance-Software.
   - Stellen Sie beim Einrichten von Web Gateway als physische Appliance mit vorinstallierter Software eine Verbindung mit der Appliance her, und schalten Sie sie ein.
   - Einrichten von Web Gateway als physische Appliance mit heruntergeladener Software:
     - Laden Sie die Software herunter, und speichern Sie sie auf einem Installationsmedium.
     - Schließen Sie die Appliance an, legen Sie das Installationsmedium ein, und schalten Sie die Appliance ein.
     - Installieren Sie die Software mithilfe des Boot-Managers.
   - Einrichten von Web Gateway als virtuelle Appliance:
     - Laden Sie die Software herunter, und speichern Sie sie auf einem Installationsmedium.
     - Legen Sie das Installationsmedium in ein geeignetes Host-System ein.
     - Erstellen Sie eine virtuelle Maschine im Host-System.
     - Starten Sie die neue virtuelle Maschine.
4 Implementieren Sie die Erstkonfigurationseinstellungen.
5 Melden Sie sich bei der Benutzeroberfläche an.
6 Lesen Sie die Online-Dokumente durch, und importieren Sie eine Lizenz.
7 Aktivieren Sie das Produkt.

Nach Abschluss der Einrichtung können Sie über die Benutzeroberfläche von Web Gateway weitere Verwaltungsaufgaben ausführen.

Informationen zum Durchführen von Upgrades für Web Gateway finden Sie in den Versionshinweisen, die mit jeder neuen Produktversion bereitgestellt werden.

Überprüfen der Anforderungen

Bevor Sie Web Gateway als physische oder virtuelle Appliance einrichten, sollten Sie sich vergewissern, dass alle Anforderungen erfüllt sind.

Anforderungen für die Einrichtung einer physischen Appliance

Für die Einrichtung einer physischen Appliance wird Folgendes benötigt:

- Im Lieferumfang enthaltene Komponenten:
  - Hardware-Plattform (unterschiedliche Modelle) mit Appliance-Software
  - Netzkabel
  - Netzwerkkabel
  - USB-PS/2-Adapterkabel (wenn Sie eine PS/2-Tastatur für die Erstkonfiguration verwenden)

Die Installationsmedien (CD/DVD und USB-Laufwerk) mit der Appliance-Software sind ebenfalls im Lieferumfang enthalten. Diese Medien sind für die Einrichtung nicht erforderlich, können aber verwendet werden, um das Appliance-Image neu zu installieren.

- Von Ihnen bereitgestellte Komponenten:
  - Standard-VGA-Monitor und PS/2-Tastatur

    oder serielle Systemkonsole
  - Administrationssystem mit:
    - Betriebssystem Windows oder Linux
    - Oracle Java Runtime Environment (JRE) 1.6 oder höher, auch als *Java 6* bezeichnet

      Aus Gründen der Web-Sicherheit beendet McAfee die Unterstützung für JRE, Version 1.6 (Java 6), nach der Veröffentlichung von Web Gateway Version 7.4.2. Genauere Informationen hierzu erhalten Sie zu einem späteren Zeitpunkt. Da JRE für die Funktion der Benutzeroberfläche erforderlich ist,

      sollten Sie von nun an JRE 1.7 (Java 7) verwenden, falls Sie diese Version nicht bereits installiert haben.
    - Microsoft Internet Explorer, Version 6.0 oder höher

      oder Mozilla Firefox, Version 2.0 oder höher
  - Netzwerkkabel für das Verwaltungssystem

Anforderungen für die Einrichtung einer virtuellen Appliance

Für die Einrichtung einer virtuellen Appliance wird Folgendes benötigt:

- Einer der folgenden VMware-Typen:
  - VMware ESX
  - VMware ESXi

    VMware Workstation, Version 5.5 oder höher, wird nicht von McAfee unterstützt, kann jedoch für Testzwecke verwendet werden.
- Host-System für virtuelle Maschinen mit den folgenden Spezifikationen:
  - CPU – 64-Bit-fähig
  - Virtualisierungserweiterung – VT-x/AMD-V
- Virtuelle Maschine mit den folgenden Spezifikationen:
  - Arbeitsspeicher – 4 GB
  - Festplattenspeicherplatz – 200 GB
  - CPU-Kerne – 2 (mindestens)

Überprüfen der standardmäßigen Erstkonfigurationseinstellungen

Sie können eine Appliance mit den standardmäßigen Erstkonfigurationseinstellungen einrichten oder eigene Einstellungen implementieren. Eigene Einstellungen legen Sie mithilfe des Konfigurations-Assistenten fest, der während des Vorgangs geöffnet wird.

In der folgenden Tabelle sind die Standardeinstellungen aufgeführt.

Tabelle 2-1 Standardmäßige Erstkonfigurationseinstellungen

Parameter	Wert
Primäre Netzwerkschnittstelle	eth0
Automatische Konfiguration mit DHCP	Ja
Host-Name	mwgappl
Root-Kennwort	<keines>
Remote-Root-Anmeldung mit SSH	Aktiviert
Standard-Gateway	<konfiguriert durch DHCP>
DNS-Server	<konfiguriert durch DHCP>

Einrichten einer physischen Appliance mit vorinstallierter Software

Auf einer neu erworbenen Hardware-Plattform ist die Appliance-Software vorinstalliert. Schließen Sie die Appliance an, und schalten Sie sie ein.

Vorgehensweise

1. Schließen Sie die Appliance an die Stromversorgung und das Netzwerk an.
2. Schließen Sie einen Monitor und eine Tastatur oder eine serielle Systemkonsole an die Appliance an.
3. Schalten Sie die Appliance ein.

   Daraufhin öffnet sich der Konfigurations-Assistent.

Nun können Sie im Konfigurations-Assistenten die Erstkonfiguration einstellen.

Siehe auch

Standardeinstellungen für eine serielle Systemkonsole auf Seite 23
Anschlusszuweisungen auf einer physischen Appliance auf Seite 23

Einrichten einer physischen Appliance mit heruntergeladener Software

Beim Einrichten einer physischen Appliance können Sie Software installieren, die Sie vom McAfee Content & Cloud Security Portal heruntergeladen haben.

Aufgaben

- *Herunterladen der Software für eine physische Appliance* auf Seite 13
  Sie können verschiedene Versionen der Appliance-Software im ISO- oder USB-Format herunterladen.
- *Installieren der heruntergeladenen Software auf einer physischen Appliance* auf Seite 13
  Zur Installation der heruntergeladenen Software auf einer physischen Appliance müssen Sie die Appliance anschließen, einschalten und mit dem Boot Manager arbeiten.

Herunterladen der Software für eine physische Appliance

Sie können verschiedene Versionen der Appliance-Software im ISO- oder USB-Format herunterladen.

Vorgehensweise

1. Navigieren Sie mit dem Browser zum McAfee Content & Cloud Security Portal unter https://contentsecurity.mcafee.com/
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort an.
3. Wählen Sie ausgehend von der Startseite des Portals **Software** | **McAfee Web Gateway 7** | **Download**.

   Daraufhin öffnet sich eine Seite mit Software-Versionen im ISO- und USB-Format.
4. Klicken Sie auf das Symbol für die genaue Software-Version, die Sie herunterladen möchten.

   Nun öffnet sich ein Download-Fenster.
5. Wählen Sie die Option zum Speichern der Datei aus, und klicken Sie auf **OK**.

   Die Software wird heruntergeladen und in Ihrem Dateisystem gespeichert.
6. Kopieren Sie die heruntergeladene Software auf eine CD/DVD oder ein USB-Laufwerk, um sie für die Installation verfügbar zu machen.

Installieren der heruntergeladenen Software auf einer physischen Appliance

Zur Installation der heruntergeladenen Software auf einer physischen Appliance müssen Sie die Appliance anschließen, einschalten und mit dem Boot Manager arbeiten.

Vorgehensweise

1. Schließen Sie die Appliance an die Stromversorgung und das Netzwerk an.
2. Schließen Sie einen Monitor und eine Tastatur oder eine serielle Systemkonsole an die Appliance an.
3. Legen Sie die CD/DVD ein, oder schließen Sie das USB-Laufwerk mit der heruntergeladenen Software an.
4. Schalten Sie die Appliance ein.

   Nun beginnt die Installation.
5. Wählen Sie während der Anfangsphase das Installationsgerät aus:
   - Wenn das Hardware-Modell Ihrer Appliance Web Gateway (WBG) 4500B, 5000B oder 5500B lautet:
     - Drücken Sie **F6**, um den Boot Manager aufzurufen.
     - Wählen Sie das Laufwerk für die CD/DVD oder das USB-Format aus, und drücken Sie dann **Enter** (Eingabe).
   - Wenn das Modell Web Gateway (WBG) 4000B lautet:
     - Drücken Sie **F2**, um das BIOS-Einrichtungsmenü aufzurufen.
     - Wählen Sie **Boot Options** (Boot-Optionen), und klicken Sie auf **Hard Disk Order** (Festplattenreihenfolge).

- Wählen Sie die Option, die dem CD/DVD- bzw. USB-Laufwerk die höchste Priorität zuweist.
- Klicken Sie auf die Registerkarte **Exit** (Beenden).
- Wählen Sie **Discard Changes** (Änderungen verwerfen).

  Verwenden Sie hier nicht die Option **Discard Changes and Exit** (Änderungen verwerfen und Beenden).

- Wählen Sie **Boot Manager** (Boot-Manager) und dann das Laufwerk für das CD/DVD- oder USB-Format aus. Drücken Sie anschließend die **Eingabetaste**.

- Sollte Ihr Modell nicht angegeben sein:
  - Drücken Sie **F11**, um den Boot Manager aufzurufen.
  - Wählen Sie das Laufwerk für die CD/DVD oder das USB-Format aus, und drücken Sie dann **Enter** (Eingabe).

Daraufhin öffnet sich das Installationsmenü auf dem Monitor.

6 Wählen Sie einen Installationsmodus aus, und drücken Sie anschließend die **Eingabetaste**.

Unterhalb des Menüs wird eine Erklärung zum jeweils ausgewählten Modus angezeigt.

Die heruntergeladene Software wird nun auf der Appliance installiert. Nach dem Abschluss der Installation öffnet sich der Konfigurations-Assistent.

Nun können Sie im Konfigurations-Assistenten die Erstkonfiguration einstellen.

Siehe auch

Standardeinstellungen für eine serielle Systemkonsole auf Seite 23
Anschlusszuweisungen auf einer physischen Appliance auf Seite 23

Einrichten einer virtuellen Appliance

Laden Sie zum Einrichten einer virtuellen Appliance die Appliance-Software vom McAfee Content & Cloud Security Portal herunter, und installieren Sie sie auf einer virtuellen Maschine.

Aufgaben

- *Herunterladen der Software für eine virtuelle Appliance* auf Seite 14
  Sie können verschiedene Versionen der Appliance-Software im ISO-Format herunterladen.
- *Installieren der heruntergeladenen Software auf einer virtuellen Appliance* auf Seite 15
  Legen Sie zum Installieren der heruntergeladenen Software auf einer virtuellen Appliance die CD/DVD mit der Software in ein geeignetes Host-System ein, erstellen Sie in diesem System eine virtuelle Maschine, und starten Sie die virtuelle Maschine.

Herunterladen der Software für eine virtuelle Appliance

Sie können verschiedene Versionen der Appliance-Software im ISO-Format herunterladen.

Vorgehensweise

1 Navigieren Sie mit dem Browser zum McAfee Content & Cloud Security Portal unter https://contentsecurity.mcafee.com/.

2 Geben Sie Ihren Benutzernamen und Ihr Kennwort an.

3 Wählen Sie ausgehend von der Startseite des Portals **Software** | **McAfee Web Gateway 7** | **Download**.

Daraufhin öffnet sich eine Seite mit Software-Versionen im ISO- und USB-Format.

4 Klicken Sie auf das ISO-Symbol für die genaue Software-Version, die Sie herunterladen möchten.

Nun öffnet sich ein Download-Fenster.

5 Wählen Sie die Option zum Speichern der Datei aus, und klicken Sie auf **OK**.

Die Software wird heruntergeladen und in Ihrem Dateisystem gespeichert.

6 Kopieren Sie die heruntergeladene Software auf eine CD/DVD, um sie für die Installation verfügbar zu machen.

Installieren der heruntergeladenen Software auf einer virtuellen Appliance

Legen Sie zum Installieren der heruntergeladenen Software auf einer virtuellen Appliance die CD/DVD mit der Software in ein geeignetes Host-System ein, erstellen Sie in diesem System eine virtuelle Maschine, und starten Sie die virtuelle Maschine.

Vorgehensweise

1 Schließen Sie eine Tastatur und einen Monitor an ein geeignetes Host-System an.

2 Legen Sie die CD/DVD mit der Appliance-Software ein.

3 Erstellen Sie mithilfe von VMware eine virtuelle Maschine im Host-System.

4 Starten Sie die neue virtuelle Maschine.

Die Appliance-Software wird auf der virtuellen Maschine installiert. Nach Abschluss dieser Installation öffnet sich der Konfigurations-Assistent auf dem Monitor des Host-Systems.

Nun können Sie im Konfigurations-Assistenten die Erstkonfiguration einstellen.

Einstellungen für virtuelle Maschinen

Beim Einrichten einer virtuellen Appliance müssen Sie Einstellungen für die virtuelle Maschine konfigurieren, die als Plattform für die Appliance-Software verwendet werden soll.

Die Vorgehensweise beim Einrichten einer virtuellen Maschine hängt vom VMware-Typ ab. Sie müssen die in der folgenden Tabelle aufgeführten Einstellungen konfigurieren.

Wenn Parameter nicht aufgelistet sind, übernehmen Sie die in den jeweiligen Abläufen angegebenen Standardwerte. Die Parameternamen können bei einzelnen Abläufen abweichen.

Tabelle 2-2 Einstellungen für virtuelle Maschinen

Option	Definition
Konfigurationstyp	Typisch | Erweitert (empfohlen für Einrichtung einer virtuellen Appliance)
Installationsmodus	Von Datenträger installieren | ISO-Image (erforderlich für Einrichtung einer virtuellen Appliance) | Später installieren
Betriebssystem	Linux (64 Bit), Version 2.6
Arbeitsspeicher	4 GB (empfohlen)
Festplatten-Speicherplatz	200 GB (empfohlen)

Tabelle 2-2 Einstellungen für virtuelle Maschinen *(Fortsetzung)*

Option	Definition
Anzahl der Prozessoren	1 | 2 (Mindestanforderung) | 4 | ... Die zur Auswahl stehende Anzahl von Prozessoren hängt von der Ausstattung des Host-Systems ab, mit dem virtuelle Appliance eingerichtet wird.
Netzwerkverbindungsmodus	Bridge (empfohlen) | NAT | ...
CD/DVD-Laufwerk mit zugewiesenem ISO-Image	<Laufwerkname>/<Name des ISO-Images>
Typ der Netzwerkschnittstellenkarte	E1000 | VMXNET 3
SCSI-Controller (für einige ESX-Versionen)	BusLogic SCSI (in 64-Bit-Umgebungen nicht unterstützt) | LSI Logic Parallel (Standard) | LSI Logic SAS | VMware PV SCSI

Implementieren der Erstkonfigurationseinstellungen

Implementieren Sie mit dem Konfigurations-Assistenten die standardmäßigen oder eigene Erstkonfigurationseinstellungen für eine Appliance.

Aufgaben

- *Implementieren der standardmäßigen Erstkonfigurationseinstellungen* auf Seite 16
  Zum Implementieren der standardmäßigen Erstkonfigurationseinstellungen konfigurieren Sie mithilfe des Assistenten ein Root-Kennwort und eine Remote-Root-Anmeldung und übernehmen die übrigen Einstellungen unverändert.
- *Implementieren eigener Einstellungen für die Erstkonfiguration* auf Seite 17
  Befolgen Sie die Anweisungen im Assistenten, um eigene Einstellungen für die Erstkonfiguration zu implementieren.

Implementieren der standardmäßigen Erstkonfigurationseinstellungen

Zum Implementieren der standardmäßigen Erstkonfigurationseinstellungen konfigurieren Sie mithilfe des Assistenten ein Root-Kennwort und eine Remote-Root-Anmeldung und übernehmen die übrigen Einstellungen unverändert.

Vorgehensweise

1 Drücken Sie als Reaktion auf sämtliche Aufforderungen des Konfigurations_Assistenten die **Esc**-Taste, bis das Root-Kennwort konfiguriert ist.

2 Wenn Sie zur Eingabe des Root-Kennworts aufgefordert werden, geben Sie es ein, und wiederholen Sie die Eingabe. Bestätigen Sie es anschließend, indem Sie auf **OK** klicken.

3 Wählen Sie bei der Frage, ob die Remote-Root-Anmeldung über SSH zulässig sein soll, nach Bedarf **Yes** (Ja) oder **No** (Nein) aus.

Wenn die Implementierung der Erstkonfigurationseinstellungen abgeschlossen sind, wird die Appliance neu gestartet, und es öffnet sich der Assistent für das Appliance-Volume, in dem Sie die Größe des Web-Caches ändern können.

Weitere Informationen hierzu finden Sie im Kapitel zur *Systemkonfiguration* im *Produkthandbuch zu McAfee Web Gateway*.

Nach Abschluss der Erstkonfiguration, mit oder ohne Änderung der Web-Cache-Größe, können Sie sich bei der Benutzeroberfläche anmelden.

Implementieren eigener Einstellungen für die Erstkonfiguration

Befolgen Sie die Anweisungen im Assistenten, um eigene Einstellungen für die Erstkonfiguration zu implementieren.

Vorgehensweise

1 Konfigurieren Sie in den Fenstern des Assistenten Folgendes:

- Primäre Netzwerkschnittstelle
- IP-Adresse, die manuell eingegeben oder dynamisch durch DHCP konfiguriert wird

Wenn Sie beabsichtigen, später den expliziten Proxy-Modus mit Hochverfügbarkeitsfunktionen (Proxy HA) zu konfigurieren, empfiehlt es sich dringend, an dieser Stelle keine virtuelle IP-Adresse einzugeben.

- Netzwerkmaske (nur nach manueller Eingabe der IP-Adresse)
- Standard-Gateway (nur nach manueller Eingabe der IP-Adresse)
- Host-Name
- DNS-Server (nur nach manueller Eingabe der IP-Adresse)

2 Überprüfen Sie die Zusammenfassung, die nach der Konfiguration der ersten Einstellungen angezeigt wird.

- Wenn die Zusammenfassung korrekt ist, bestätigen Sie sie, und konfigurieren Sie dann die verbleibenden Einstellungen:
  - Root-Kennwort
  - Remote-Root-Anmeldung mit SSH

  Der Installationsvorgang wird mit Ihren Erstkonfigurationseinstellungen abgeschlossen, und die IP-Adresse wird angezeigt.

  Sie können sich jetzt bei der Benutzeroberfläche anmelden.
- Falls Sie Änderungen vornehmen müssen, klicken Sie auf **Cancel** (Abbrechen), und kehren Sie zu Schritt 1 zurück.

Wenn die Implementierung der Erstkonfigurationseinstellungen abgeschlossen sind, wird die Appliance neu gestartet, und es öffnet sich der Assistent für das Appliance-Volume, in dem Sie die Größe des Web-Caches ändern können.

Weitere Informationen hierzu finden Sie im Kapitel zur *Systemkonfiguration* im *Produkthandbuch zu McAfee Web Gateway*.

Nach Abschluss der Erstkonfiguration, mit oder ohne Änderung der Web-Cache-Größe, können Sie sich bei der Benutzeroberfläche anmelden.

Anmelden bei der Benutzeroberfläche

Sie können sich in einem Browser auf Ihrem Administrationssystem bei der Benutzeroberfläche von Web Gateway anmelden.

Vorgehensweise

1 Öffnen Sie den Browser, und navigieren Sie zu einer der folgenden Adressen:

- `http://<IP-Adresse>:4711`
- `https://<IP-Adresse>:4712`

`<IP-Adresse>` ist hierbei die IP-Adresse der Erstkonfiguration.

> Stimmen Sie unter HTTPS dem selbstsignierten Zertifikat zu, das angezeigt wird.

Nun öffnet sich ein Anmeldefenster.

2 Geben Sie als Benutzername `admin` und als Kennwort `webgateway` ein.

Nach einer erfolgreichen Anmeldung öffnet sich der Einrichtungs-Assistent.

Arbeiten mit dem Einrichtungs-Assistenten

Mit dem Einrichtungs-Assistenten aktivieren Sie das Produkt und führen die gesamte Einrichtung durch.

Aufgaben

- *Aktivieren des Produkts* auf Seite 18
  Lesen Sie sich zur Aktivierung des Produkts die beiden Online-Dokumente zur Lizenzierung und Datennutzung durch. Importieren Sie anschließend eine Lizenz, und klicken Sie auf die Aktivierungsschaltfläche.
- *Konfigurieren weiterer Ersteinstellungen* auf Seite 20
  Bei der Ersteinstellung werden die Zeitzone, die Netzwerkschnittstellen und der DNS-Server konfiguriert.
- *Beheben von Problemen durch Herstellen einer Verbindung mit den Download-Servern* auf Seite 21
  Führen Sie diese Prozedur durch, wenn der nach der Aktivierung des Produkts gestartete Download aufgrund von Problemen beim Herstellen einer Verbindung mit den Download-Servern fehlschlägt.

Aktivieren des Produkts

Lesen Sie sich zur Aktivierung des Produkts die beiden Online-Dokumente zur Lizenzierung und Datennutzung durch. Importieren Sie anschließend eine Lizenz, und klicken Sie auf die Aktivierungsschaltfläche.

> Sie müssen den Inhalten der Online-Dokumente zustimmen, um das Produkt aktivieren zu können.

Für die Lizenzierung wurde Ihnen eine Datei mit einem Lizenzschlüssel zugesendet. Falls Sie diese nicht erhalten haben, wenden Sie sich an den McAfee-Support. In der Zwischenzeit können Sie einen temporären Schlüssel verwenden.

Vorgehensweise

1 Klicken Sie im Abschnitt **License** (Lizenz) des Einrichtungs-Assistenten auf **End User License Agreement** (Endbenutzer-Lizenzvertrag), und lesen Sie den Vertrag. Wenn Sie den Bestimmungen zustimmen, aktivieren Sie das entsprechende Kontrollkästchen.

2 Klicken Sie auf **Data Usage Statement** (Datennutzungserklärung), und lesen Sie die Erklärung. Wenn Sie den Bestimmungen zustimmen, aktivieren Sie das entsprechende Kontrollkästchen.

3 Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie im daraufhin geöffneten Datei-Manager die Datei mit dem Lizenzschlüssel aus. Klicken Sie anschließend auf **OK**.

Daraufhin wird die Schaltfläche **Activate product** (Produkt aktivieren) aktiviert.

4 Klicken Sie auf **Activate product** (Produkt aktivieren).

Web Gateway wird nun aktiviert, und es werden die Dateien heruntergeladen, mit denen die von den Anti-Malware- und URL-Filterungsmodulen verwendeten Daten aktualisiert werden.

Der Download-Fortschritt wird durch einen Fortschrittsbalken unten auf der Seite angezeigt und durch eine Statusbezeichnung erläutert.

5 Führen Sie einen der folgenden Vorgänge aus:

- Warten Sie, bis der Download erfolgreich beendet wurde, und klicken Sie dann auf **Close wizard** (Assistent schließen).

  Damit ist die Einrichtung abgeschlossen. Sie können nun mit der Benutzeroberfläche arbeiten und weitere Verwaltungsmaßnahmen durchführen.

  Bei Bedarf können Sie die Einstellungen für die Datenerfassung konfigurieren und anschließend auf **Save Changes** (Änderungen speichern) klicken. Weitere Informationen hierzu finden Sie in der *Datennutzungserklärung*.

  Klicken Sie nicht auf **Save Changes** (Änderungen speichern), um andere Einstellungen zu speichern (falls Sie dies vorhaben), bevor Sie die Datenerfassung konfiguriert haben, da die Datenerfassung beginnt, wenn Sie zum ersten Mal auf diese Schaltfläche klicken.

  Weitere Informationen zum Arbeiten mit der Benutzeroberfläche finden Sie im *Produkthandbuch zu McAfee Web Gateway*.

- Konfigurieren Sie weitere Ersteinstellungen.

  Der Download-Fortschritt bleibt sichtbar, während Sie den Assistenten durchlaufen.

Falls beim Herunterladen ein Fehler auftritt, wird eine Fehlermeldung angezeigt, und Sie können dann auf den Abschnitt **Network solutions** (Netzwerklösungen) im Navigationsbereich zugreifen. Dort können Sie Probleme beim Herstellen einer Verbindung mit den Download-Servern beheben.

Siehe auch

Aktivieren von Web Gateway mit einem temporären Lizenzschlüssel auf Seite 22

Konfigurieren weiterer Ersteinstellungen

Bei der Ersteinstellung werden die Zeitzone, die Netzwerkschnittstellen und der DNS-Server konfiguriert.

Sie können diese Einstellungen später über die Benutzeroberfläche konfigurieren. Wählen Sie im übergeordneten Menü **Configuration** (Konfiguration) die Optionen **Date and Time** (Datum und Uhrzeit), **Network Interfaces** (Netzwerkschnittstellen) oder **Domain Name Service** (Domänennamen-Dienst) aus.

Wählen Sie zum Festlegen von Administrator-Kennwörtern **Accounts** | **Administrator Accounts** (Konten | Administrator-Konten) aus.

Vorgehensweise

1. Wählen Sie im Abschnitt **Time Zone** (Zeitzone) des Assistenten eine Zeitzone für die Web Gateway-Appliance aus, oder übernehmen Sie die Standardzone (UTC).
2. Konfigurieren Sie im Abschnitt **Network settings** (Netzwerkeinstellungen) auf der Registerkarte **Network interfaces** (Netzwerkschnittstellen) die folgenden Optionen:
   - Geben Sie im Feld **Host name / Fully qualified domain name** (Host-Name / Vollqualifizierter Domänenname) einen Host-Namen für die Appliance ein.
   - Geben Sie im Feld **Default gateway (IPv4)** (Standard-Gateway (IPv4)) oder **Default gateway (IPv6)** (Standard-Gateway (IPv6)) eine IP-Adresse im IPv4- bzw. IPv6-Format ein.

     Wählen Sie zur dynamischen Konfiguration der Standard-Gateway-Adresse unter **IP settings** (IP-Einstellungen) die Option **Obtain automatically (DHCP)** (Automatisch beziehen (DHCP)) aus.
3. Geben Sie im Abschnitt **Network settings** (Netzwerkeinstellungen) auf der Registerkarte **Domain name servers** (Domänennamen-Server) die IP-Adressen für bis zu drei DNS-Server ein.
4. [Optional] Ändern Sie im Abschnitt **Password** (Kennwort) das vorkonfigurierte Administrator-Kennwort.
5. Klicken Sie auf **Close wizard** (Assistent schließen).

   Daraufhin wird der Assistent geschlossen, und Sie können auf die Benutzeroberfläche zugreifen. Sie werden dann in einer Meldung gefragt, ob Sie die Konfiguration speichern möchten.
6. Führen Sie einen der folgenden Vorgänge aus:
   - Wenn Sie ebenfalls Einstellungen für Datensammlungen konfigurieren möchten, dann konfigurieren Sie diese, und klicken Sie anschließend auf **Save Changes** (Änderungen speichern). Weitere Informationen hierzu finden Sie in der *Datennutzungserklärung*.
   - Klicken Sie jetzt auf **Save Changes** (Änderungen speichern).

Beheben von Problemen durch Herstellen einer Verbindung mit den Download-Servern

Führen Sie diese Prozedur durch, wenn der nach der Aktivierung des Produkts gestartete Download aufgrund von Problemen beim Herstellen einer Verbindung mit den Download-Servern fehlschlägt.

Vorgehensweise

1 Führen Sie im Abschnitt **Network solutions** (Netzwerklösungen) des Assistenten je nach dem vorliegenden Problem einen der folgenden Schritte aus.

- Falls die Download-Server nicht zum Aktualisieren der Filterinformationen verwendet werden können, da Sie die Appliance in einer Umgebung ohne Internet-Verbindung ausführen, klicken Sie auf **Perform offline update** (Offline-Update ausführen).
- Wenn Sie einen Proxy des nächsten Hops zum Herstellen einer Verbindung zu den Download-Servern verwenden möchten, dann klicken Sie auf **Specify next-hop proxy for download** (Proxy des nächsten Hops für Download angeben), und fahren Sie mit Schritt 2 fort.
- Wenn Sie den Domain Name Service ändern möchten, bevor Sie eine Verbindung mit den Download-Servern herstellen, dann klicken Sie auf **Specify DNS servers for download** (DNS-Server für Download angeben), und fahren Sie mit Schritt 3 fort.

2 Konfigurieren Sie unter **Next Hop Proxy Definition** (Proxy-Definition des nächsten Hops) die folgenden Optionen:

a Geben Sie im Feld **Host** einen Host-Namen oder eine IP-Adresse für den Proxy des nächsten Hops im IPv4- oder IPv6-Format ein.

b Geben Sie im Feld **Port** eine Port-Nummer für den Port am Proxy des nächsten Hops ein, der auf die Aufforderungen von Web Gateway reagiert.

c Geben Sie im Feld **User** (Benutzer) den Benutzernamen ein, den Web Gateway bei der Authentifizierung an den Proxy des nächsten Hops sendet.

d Geben Sie im Feld **Password** (Kennwort) das Kennwort ein, das Web Gateway bei der Authentifizierung an den Proxy des nächsten Hops sendet.

e Klicken Sie auf **Continue** (Weiter).

Der Assistent schließt den Abschnitt **Network solutions** (Netzwerklösungen) und kehrt zur Hauptseite zurück. Wenn Sie auch den Domain Name Service ändern möchten, dann fahren Sie mit Schritt 3 fort, ansonsten fahren Sie mit Schritt 4 fort.

3 Konfigurieren Sie unter **Domain Name Server Configuration** (Domänennamenserver-Konfiguration) die folgenden Optionen:

a Geben Sie in den Feldern unter **Domain name server** (DNS-Server) die IP-Adressen für bis zu drei DNS-Server ein.

b Klicken Sie auf **Continue** (Weiter).

Der Assistent schließt den Abschnitt **Network solutions** (Netzwerklösungen) und kehrt zur Hauptseite zurück.

4 Klicken Sie auf **Retry download of engines and patterns** (Download von Engines und Mustern wiederholen).

Der Download wird nun abgeschlossen. Falls der Download noch immer nicht erfolgreich abgeschlossen werden kann, schließen Sie den Assistenten, und versuchen Sie, das Problem anderweitig zu lösen.

Aktivieren von Web Gateway mit einem temporären Lizenzschlüssel

Wenn Sie von McAfee keine Datei mit einem Lizenzschlüssel erhalten haben, können Sie Web Gateway mit einem temporären Schlüssel aktivieren.

Mit der Aktivierungs-ID, die sich auf einem Etikett auf Ihrer Appliance-Verpackung befindet, können Sie diesen Schlüssel generieren. Beispiel: *Aktivierungs-ID: 0923839534*

Vorgehensweise

1. Navigieren Sie mit dem Browser zum McAfee Content & Cloud Security Portal unter https://contentsecurity.mcafee.com/.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort an.
3. Geben Sie auf der Startseite des Portals hinter der in Schritt 1 angegebenen URL `activate` ein, und drücken Sie anschließend die **Eingabetaste**.

   Daraufhin öffnet sich die Seite **Activation** (Aktivierung).
4. Geben Sie im Feld **Activation ID** (Aktivierungs-ID) die Aktivierungs-ID vom Etikett auf Ihrer Appliance-Verpackung ein, und klicken Sie anschließend auf **Activate** (Aktivieren).
5. Befolgen Sie nun die angezeigten Online-Anweisungen.

Aufspielen eines neuen Images auf eine Appliance

Verwenden Sie zum Aufspielen eines neuen Images auf eine Appliance die Appliance-Software auf der CD/DVD oder dem im Lieferumfang enthaltenen USB-Laufwerk.

Statt zum Aufspielen des Images die Appliance-Software auf dem mitgelieferten Medium zu nutzen, können Sie die Software für das Aufspielen des Images über das McAfee Content & Cloud Security Portal herunterladen und für diesen Zweck auf ein USB-Laufwerk kopieren.

Das USB-Laufwerk muss bootfähig sein, damit es zum Aufspielen eines neuen Images verwendet werden kann. Sie können ein bootfähiges USB-Laufwerk mit einem entsprechenden Programm erstellen, beispielsweise mit Microsoft Win32diskimager.

Beim Aufspielen eines neuen Images auf eine Appliance werden alle zuvor darauf gespeicherten Daten überschrieben.

Vorgehensweise

1. Sichern Sie die Konfiguration der Appliance über die Benutzeroberfläche von Web Gateway anhand der Funktionen unter **Troubleshooting** | **Backup/Restore** (Fehlerbehebung | Sichern/Wiederherstellen).
2. Schließen Sie einen Monitor und eine Tastatur an die Appliance an.
3. Legen Sie die CD/DVD ein, bzw. schließen Sie das USB-Laufwerk an die Appliance an.
4. Schalten Sie die Appliance ein.
5. Drücken Sie bei einer entsprechenden Aufforderung **F2**, um das Einrichtungsmenü aufzurufen.

6 Wählen Sie **Boot manager** (Boot-Manager) und anschließend die Option für das CD/DVD- bzw. USB-Laufwerk aus. Drücken Sie anschließend die **Eingabetaste**.

> Bei einigen Appliance-Modellen können Sie auch **F6** drücken, um das Boot-Manager-Menü direkt aufzurufen.

Daraufhin öffnet sich das Installationsmenü auf dem Monitor.

7 Wählen Sie einen Installationsmodus aus, und drücken Sie anschließend die **Eingabetaste**.

> Unterhalb des Menüs wird eine Erklärung zum jeweils ausgewählten Modus angezeigt.

Die heruntergeladene Software wird nun auf der Appliance installiert. Nach dem Abschluss der Installation öffnet sich der Konfigurations-Assistent.

Nun können Sie im Konfigurations-Assistenten die Erstkonfiguration einstellen.

Standardeinstellungen für eine serielle Systemkonsole

Beim Herstellen der Verbindung einer seriellen Systemkonsole mit einer Web Gateway-Appliance für Verwaltungszwecke gelten die folgenden Standardeinstellungen.

Tabelle 2-3 Standardeinstellungen für serielle Konsolen

Parameter	Wert
Baud-Rate	19200
Daten-Bits	8
Paritäts-Bit	N (kein)
Stopp-Bits	1
Kurz	19200/8-N-1
Flusssteuerung	keine

Anschlusszuweisungen auf einer physischen Appliance

Nach der Einrichtung der physischen Appliance werden den Netzwerkschnittstellen in der Appliance-Hardware Anschlüsse zugewiesen.

Folgende Modelle der Appliance-Hardware sind verfügbar:

- WBG-4000-B
- WBG-4500-B
- WBG-4500-C
- WBG-5000-B
- WBG-5000-C
- WBG-5500-B
- WBG-5500-C

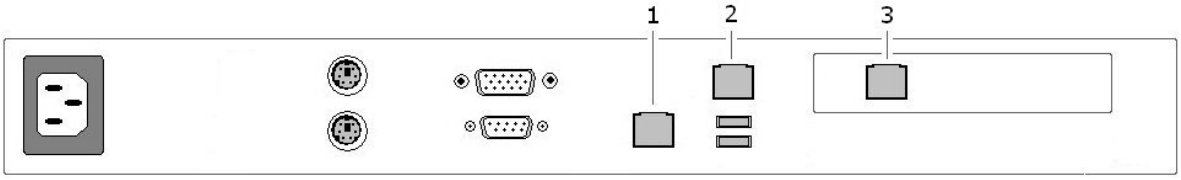
Die Modellnummer befindet sich auf einem Etikett oben auf dem Hardware-Chassis.

Die Abbildungen in den folgenden Abschnitten veranschaulichen die Anschlusszuweisungen für die verschiedenen Appliance-Modelle und die vom Betriebssystem für die Netzwerkschnittstellen verwendeten Namen.

Nach der Installation einer Glasfaser-Netzwerkschnittstellenkarte sind weitere Netzwerkschnittstellen verfügbar.

WBG-4000-B

Dieses Appliance-Modell verfügt an der Rückseite über drei Netzwerkschnittstellen.



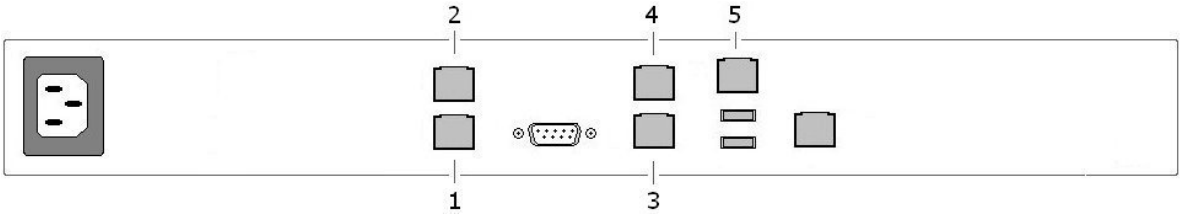
Anschlüsse und Namen für diese Schnittstellen:

Position	Netzwerkschnittstelle mit Anschluss	Schnittstellenname des Betriebssystems
1	e1000e	eth0
2	e1000	eth1
3	e1000e	eth2

An der *Vorderseite* dieses Appliance-Modells leuchtet die Leuchtanzeige für Netzwerkschnittstelle 2 auf, wenn Netzwerkschnittstelle 1 angeschlossen wird. Wenn Netzwerkschnittstelle 2 angeschlossen wird, leuchtet die Leuchtanzeige für Netzwerkschnittstelle 1 auf.

WBG-4500-B

Dieses Appliance-Modell verfügt an der Rückseite über fünf Netzwerkschnittstellen.

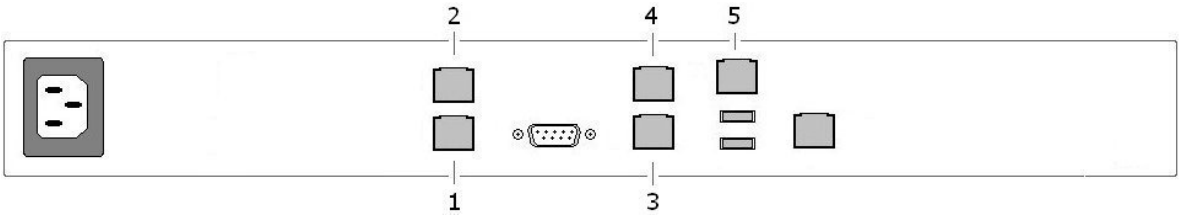


Anschlüsse und Namen für diese Schnittstellen:

Position	Netzwerkschnittstelle mit Anschluss	Schnittstellenname des Betriebssystems
1	igb	eth0
2	igb	eth1
3	igb	eth2
4	igb	eth3
5	e1000e	eth4

WBG-4500-C

Dieses Appliance-Modell verfügt an der Rückseite über fünf Netzwerkschnittstellen.

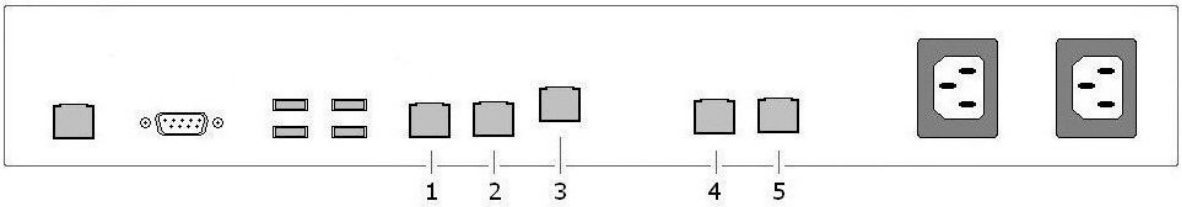


Anschlüsse und Namen für diese Schnittstellen:

Position	Netzwerkschnittstelle mit Anschluss	Schnittstellenname des Betriebssystems
1	igb	eth0
2	igb	eth1
3	igb	eth2
4	igb	eth3
5	e1000e	eth4

WBG-5000-B

Dieses Appliance-Modell verfügt an der Rückseite über fünf Netzwerkschnittstellen.

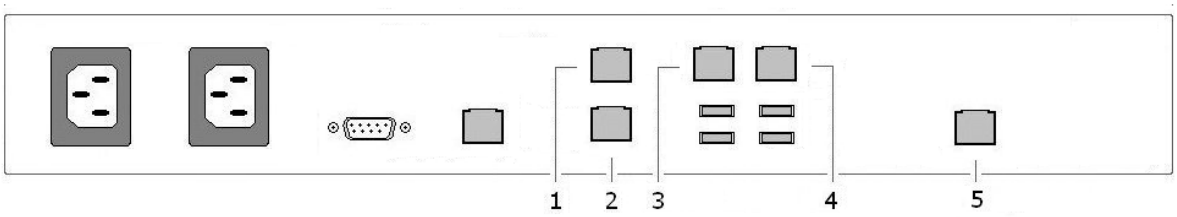


Anschlüsse und Namen für diese Schnittstellen:

Position	Netzwerkschnittstelle mit Anschluss	Schnittstellenname des Betriebssystems
1	igb	eth0
2	igb	eth1
3	rmm und bmc Für den Betrieb von RMM (Remote Management Module) und BMC (Baseboard Management Controller)	
4	e1000e	eth3
5	e1000e	eth2

WBG-5000-C

Dieses Appliance-Modell verfügt an der Rückseite über fünf Netzwerkschnittstellen.

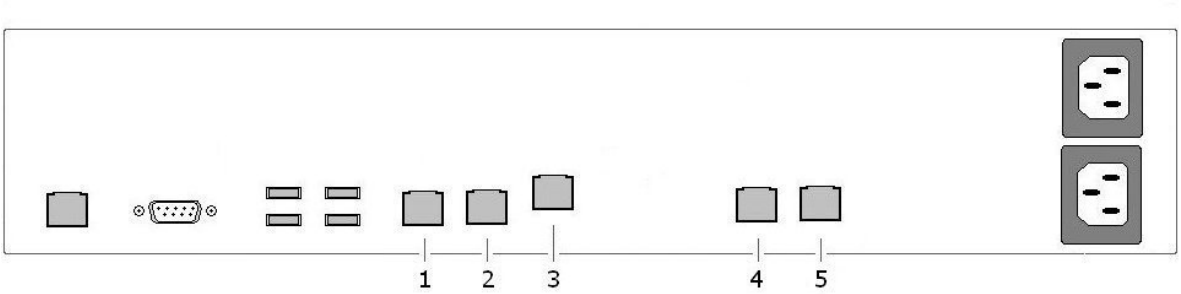


Anschlüsse und Namen für diese Schnittstellen:

Position	Netzwerkschnittstelle mit Anschluss	Schnittstellenname des Betriebssystems
1	igb	eth0
2	igb	eth1
3	igb	eth2
4	igb	eth3
5	rmm und bmc Für den Betrieb von RMM (Remote Management Module) und BMC (Baseboard Management Controller)	

WBG-5500-B

Dieses Appliance-Modell verfügt an der Rückseite über fünf Netzwerkschnittstellen.

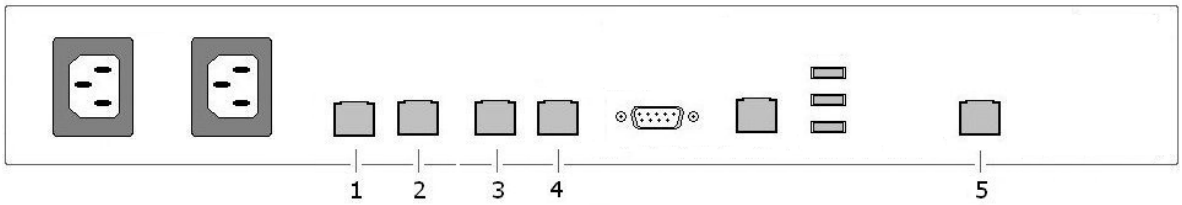


Anschlüsse und Namen für diese Schnittstellen:

Position	Netzwerkschnittstelle mit Anschluss	Schnittstellenname des Betriebssystems
1	igb	eth0
2	igb	eth1
3	rmm und bmc Für den Betrieb von RMM (Remote Management Module) und BMC (Baseboard Management Controller)	
4	e1000e	eth3
5	e1000e	eth2

WBG-5500-C

Dieses Appliance-Modell verfügt an der Rückseite über fünf Netzwerkschnittstellen.



Anschlüsse und Namen für diese Schnittstellen:

Position	Netzwerkschnittstelle mit Anschluss	Schnittstellenname des Betriebssystems
1	igb	eth0
2	igb	eth1
3	igb	eth2
4	igb	eth3
5	rmm und bmc Für den Betrieb von RMM (Remote Management Module) und BMC (Baseboard Management Controller)	

3 Installieren einer PCI-Karte

PCI-Karten (Peripheral Component Interconnect) können auf einer Web Gateway-Appliance beispielsweise installiert werden, um Glasfaserverbindungen oder die Nutzung eines HSM (Hardware Security Module) zu ermöglichen.

Inhalt

- *Unterstützte HSM-Karten*
- *Unterstützte Glasfaser-Netzwerkschnittstellenkarten*
- *Installieren einer PCI-Karte*

Unterstützte HSM-Karten

Ein Hardware Security Module (HSM) wird auf einer als *HSM-Karte* bezeichneten PCI-Karte bereitgestellt. Wenn Sie die Funktionen dieses Moduls auf einer Web Gateway-Appliance nutzen möchten, müssen Sie im Fachhandel eine geeignete HSM-Karte erwerben und installieren.

McAfee unterstützt nur die im vorliegenden Handbuch aufgeführten HSM-Karten.

Die folgenden Karten oder entsprechende Modelle können installiert werden.

Tabelle 3-1 Unterstützte HSM-Kartentypen

Anbieter	Typ	Untertyp	Höhe
Thales	nCipher nShield	500e F3	Volle Höhe

Weitere Informationen zur Arbeit mit einem Hardware Security Module finden Sie im Kapitel *Web-Filterung* des *Produkthandbuchs zu McAfee Web Gateway*.

Unterstützte Glasfaser-Netzwerkschnittstellenkarten

Glasfaser-Netzwerkschnittstellenkarten sind PCI-Karten, die Glasfaserverbindungen ermöglichen. Wenn Sie auf einer Web Gateway-Appliance Glasfaserverbindungen bereitstellen möchten, müssen Sie im Fachhandel eine geeignete Glasfaser-Netzwerkschnittstellenkarte erwerben und installieren.

Es werden 1GbE- und 10GbE-Karten unterstützt. Bei Verwendung einer 10GbE-Glasfaser-Netzwerkschnittstellenkarte müssen Sie außerdem im Fachhandel einen Transceiver (auch als *GBIC* bezeichnet) erwerben und installieren.

McAfee unterstützt nur die im vorliegenden Handbuch aufgeführten Glasfaser-Netzwerkschnittstellenkarten und Transceiver.

Die folgenden Karten können installiert werden:

Tabelle 3-2 Unterstützte Typen von 1GbE- und 10GbE-Glasfaser-Netzwerkschnittstellenkarten

Anbieter	Typ	Untertyp	Medium	Anschlüsse	Höhe
Intel	i340-F4	E1G44HT	1000BASE-SX	4	Voll
HotLava	Tambora 64G4	4ST2830A2	10GBASE-SR Erforderlicher Transceiver (GBIC): HLSR10G3A SFP+ HotLava-Module/Optik	4	Halbhoch mit montierter Vollprofil-Halterung
HotLava	Tambora 80G4S-G3	4ST3830A1F	10GBASE-SR Erforderlicher Transceiver (GBIC): HLSR10G4A SFP+ HotLava-Module/Optik	4	Halbhoch mit montierter Vollprofil-Halterung

Die Karten können in den folgenden Web Gateway-Appliance-Modellen installiert werden:

Tabelle 3-3 Geeignete Web Gateway-Appliance-Modelle

Modell	Höheneinheiten	Steckplätze
WBG-5000-B	1	1 x PCI, volle Höhe
WBG-5000-C	1	1 x PCI, volle Höhe
WBG-5500-B	2	2 x PCI, niedriges Profil 3 x PCI, volle Höhe
WBG-5500-C	1	2 x PCI, volle Höhe

Die Modelle WBG-5000-B und WBG-5000-C enthalten nur einen Slot zum Einsetzen einer PCI-Karten. Die Modelle WBG-5500-B und WBG-5500-C enthalten zwei Slots, sodass Sie eine HSM-Karte und eine Glasfaserkarte installieren können.

Konfigurationen mit mehreren Glasfaserkarten in einer Appliance wurden von McAfee bisher nicht getestet.

1GbE-Glasfaser-Netzwerkschnittstellenkarte

Auf einer Web Gateway-Appliance werden 1GbE-Glasfaser-Netzwerkschnittstellenkarten vom Typ *Intel i340-F4* unterstützt.

Diese Glasfaserkarte ist mit vier optischen Anschlüssen ausgestattet und unterstützt 1000BASE-SX-Medien mit LC-Anschlüssen. Es handelt sich um eine PCIe-Karte mit voller Bauhöhe.

Die Anschlüsse für die Schnittstellen auf der vorhandenen Onboard-Netzwerkschnittstellenkarte und der Glasfaserkarte sind den Schnittstellennamen, die vom MLOS-Betriebssystem verwenden werden, wie folgt zugeordnet.

Tabelle 3-4 Anschlusszuordnung mit installierter 1GbE-Glasfaserkarte

Anschluss auf Onboard- oder Glasfaser-Netzwerkschnittstellenkarte	Schnittstellenname des Betriebssystems
Onboard-Netzwerkschnittstellenkarte Anschluss 1	eth0
Onboard-Netzwerkschnittstellenkarte Anschluss 2	eth1

Tabelle 3-4 Anschlusszuordnung mit installierter 1GbE-Glasfaserkarte *(Fortsetzung)*

Anschluss auf Onboard- oder Glasfaser-Netzwerkschnittstellenkarte	Schnittstellenname des Betriebssystems
Onboard-Netzwerkschnittstellenkarte Anschluss 3	eth2
Onboard-Netzwerkschnittstellenkarte Anschluss 4	eth3
1GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 1 (ganz rechts)	eth4
1GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 2	eth5
1GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 3	eth6
1GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 4 (ganz links)	eth7

Im Vergleich zu ihrer Position auf der Rückseite der Appliance sind die Anschlüsse auf der Glasfaserkarte und entsprechend auch ihre Schnittstellennamen in umgekehrter Reihenfolge nummeriert.

Von links nach rechts lautet die Reihenfolge der Schnittstellennamen wie folgt:

```
eth7 – eth6 – eth5 – eth4
```

Auf der Rückseite des Modells WBG-5000-B lautet die Reihenfolge der Schnittstellennamen beispielsweise wie folgt:

Abbildung 3-1 Schnittstellennamen für Anschlüsse der 1GbE-Glasfaserkarte auf Modell WBG-5000-B

Auf der Rückseite des Modells WBG-5500-B lautet die Reihenfolge wie folgt:

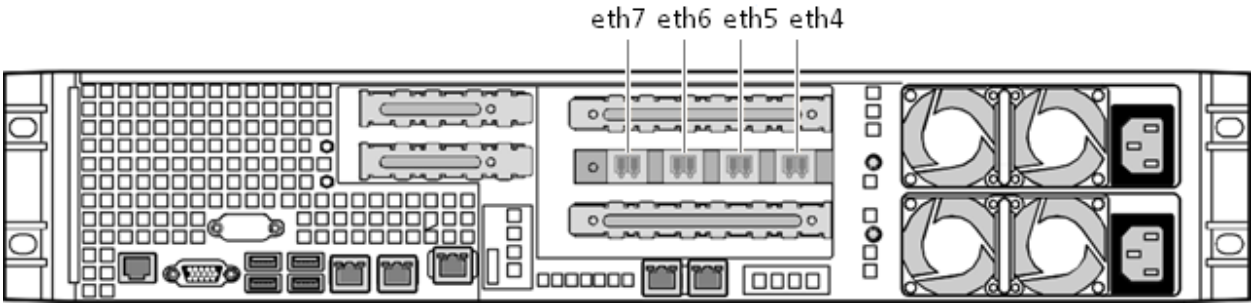


Abbildung 3-2 Schnittstellennamen für Anschlüsse der 1GbE-Glasfaserkarte auf Modell WBG-5500-B

Auf der Rückseite des Modells WBG-5000-C lautet die Reihenfolge wie folgt:

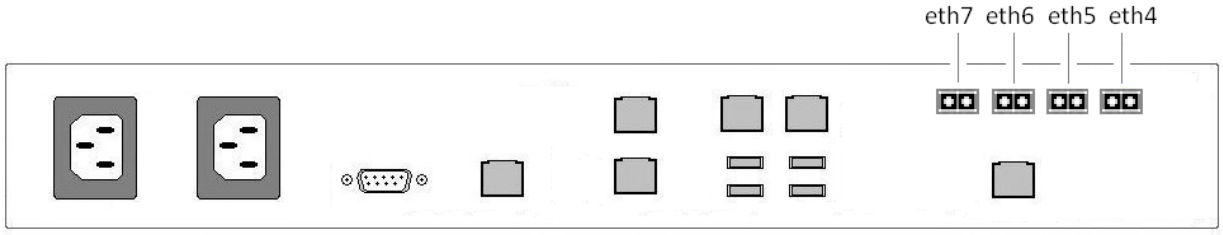


Abbildung 3-3 Schnittstellennamen für Anschlüsse der 1GbE-Glasfaserkarte auf der Rückseite des Modells WBG-5000-C

Auf der Rückseite des Modells WBG-5500-C lautet die Reihenfolge wie folgt:

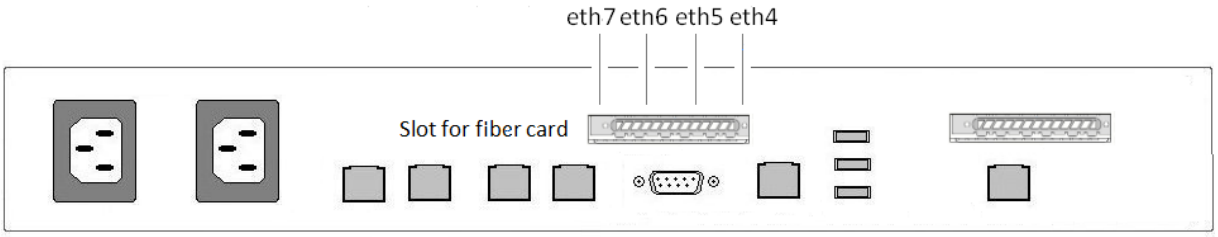


Abbildung 3-4 Schnittstellennamen für Anschlüsse der 1GbE-Glasfaserkarte auf der Rückseite des Modells WBG-5500-C

Das Modell WBG-5500-C enthält zwei Slots zum Einsetzen von PCI-Karten. Setzen Sie die Glasfaserkarte in den oben markierten Slot ein.

10GbE-Glasfaser-Netzwerkschnittstellenkarte

Auf einer Web Gateway-Appliance werden 10GbE-Glasfaser-Netzwerkschnittstellenkarten vom Typ *HotLava Tambora 64G4* und *HotLava Tambora 80G4S-G3*unterstützt.

Dies sind halbhohe PCIe-Karten, die standardmäßig mit einer Halterung in voller Höhe versehen sind, die mit der Halterungshöhe der Web Gateway-Appliance-Modelle kompatibel ist.

Wenn Sie eine Glasfaserkarte dieses Typs verwenden möchten, müssen Sie auch folgenden Transceiver mit GBIC-Komponenten installieren: 4 HotLava HLSR10G3A SFP+ Module/Optik für 10GBASE-SR-Medien mit LC-Anschlüssen.

Die Anschlüsse für die Schnittstellen auf der vorhandenen Onboard-Netzwerkschnittstellenkarte und der Glasfaserkarte sind den Schnittstellennamen, die vom MLOS-Betriebssystem verwenden werden, wie folgt zugeordnet.

Tabelle 3-5 Anschlusszuordnung mit installierter 10GbE-Glasfaserkarte

Anschluss auf Onboard- oder Glasfaser-Netzwerkschnittstellenkarte	Schnittstellenname des Betriebssystems
Onboard-Netzwerkschnittstellenkarte Anschluss 1	eth0
Onboard-Netzwerkschnittstellenkarte Anschluss 2	eth1
Onboard-Netzwerkschnittstellenkarte Anschluss 3	eth2
Onboard-Netzwerkschnittstellenkarte Anschluss 4	eth3
10GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 1 (ganz links)	eth4
10GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 2	eth5

Tabelle 3-5 Anschlusszuordnung mit installierter 10GbE-Glasfaserkarte *(Fortsetzung)*

Anschluss auf Onboard- oder Glasfaser-Netzwerkschnittstellenkarte	Schnittstellenname des Betriebssystems
10GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 3	eth6
10GbE-Glasfaser-Netzwerkschnittstellenkarte Anschluss 4 (ganz rechts)	eth7

Im Vergleich zu ihrer Position auf der Rückseite der Appliance sind die Anschlüsse auf der Glasfaserkarte und entsprechend auch ihre Schnittstellennamen in der üblichen Reihenfolge nummeriert.

Von links nach rechts lautet die Reihenfolge der Schnittstellennamen wie folgt:

```
eth4 – eth5 – eth6 – eth7
```

Auf der Rückseite des Modells WBG-5000-B lautet die Reihenfolge der Schnittstellennamen beispielsweise wie folgt:

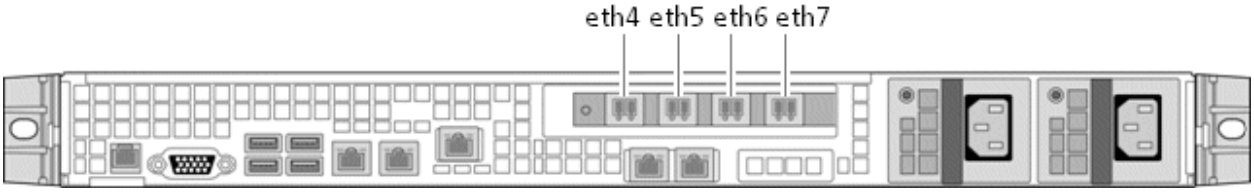


Abbildung 3-5 Schnittstellennamen für Anschlüsse der 10GbE-Glasfaserkarte auf der Rückseite des Modells WBG-5000-B

Auf der Rückseite des Modells WBG-5500-B lautet die Reihenfolge wie folgt:

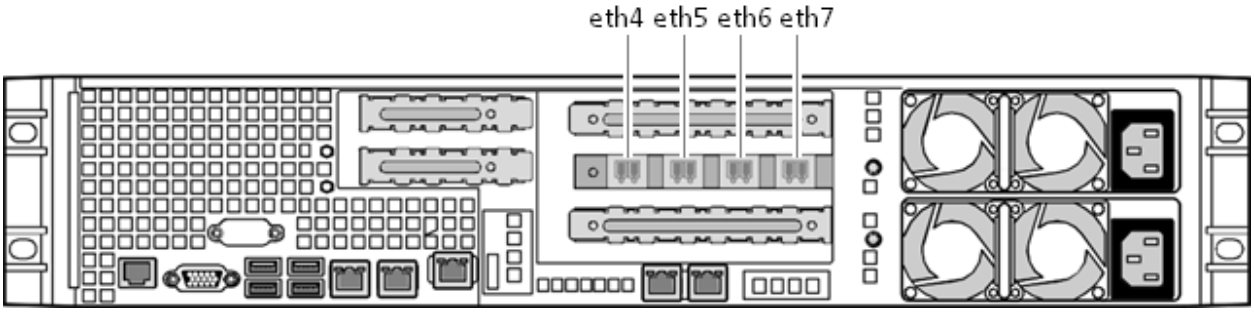


Abbildung 3-6 Schnittstellennamen für Anschlüsse der 10GbE-Glasfaserkarte auf der Rückseite des Modells WBG-5500-B

Auf der Rückseite des Modells WBG-5000-C lautet die Reihenfolge wie folgt:

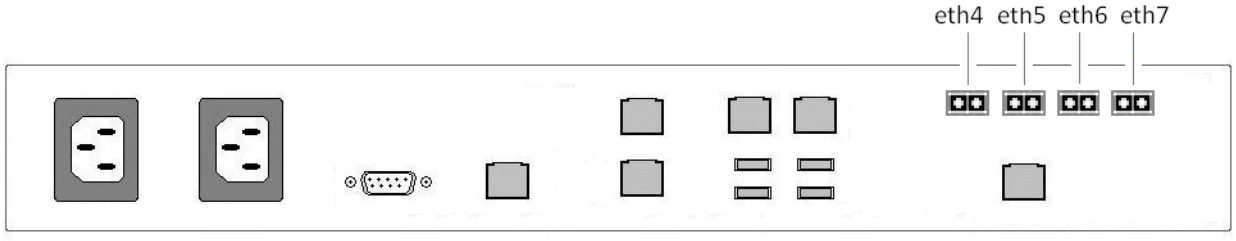


Abbildung 3-7 Schnittstellennamen für Anschlüsse der 10GbE-Glasfaserkarte auf der Rückseite des Modells WBG-5000-C

Auf der Rückseite des Modells WBG-5500-C lautet die Reihenfolge wie folgt:

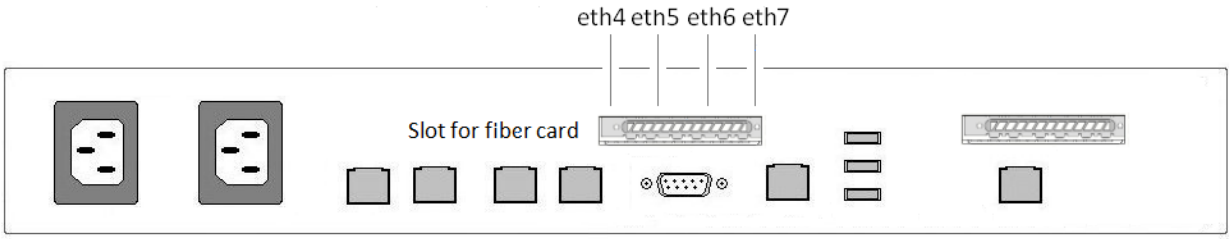


Abbildung 3-8 Schnittstellennamen für Anschlüsse der 10GbE-Glasfaserkarte auf der Rückseite des Modells WBG-5500-C

Das Modell WBG-5500-C enthält zwei Slots zum Einsetzen von PCI-Karten. Setzen Sie die Glasfaserkarte in den oben markierten Slot ein.

Installieren einer PCI-Karte

Zum Installieren einer PCI-Karte auf einer Web Gateway-Appliance müssen Sie die Appliance vom Netzwerk trennen, die Abdeckung abnehmen und die Karte dann in einen geeigneten Slot einsetzen.

Sie sollten unbedingt in einem ESD-geschützten Bereich arbeiten, damit die Appliance und die PCI-Karte nicht durch elektrostatische Entladungen beschädigt werden.

Bei einigen Appliance-Modellen (z. B. WBG-5000-B) ist die PCI-Karte mit einer Schraube fixiert, bei anderen (z. B. WBG-5500-B) mit Haltefedern.

Vorgehensweise

1 Schalten Sie die Appliance aus, und ziehen Sie das Netzkabel ab.

2 Nehmen Sie die Abdeckung der Appliance ab.

Schalten Sie die Appliance aus, und ziehen Sie das Netzkabel ab, *bevor* Sie die Abdeckung abnehmen. Andernfalls besteht die Gefahr eines elektrischen Schlags, und die Appliance sowie die PCI-Karte könnten beschädigt werden.

3 Setzen Sie die PCI-Karte ein.

a Nehmen Sie die PCI-Riser-Komponente heraus.

b Wenn die PCI-Karte mit Haltefedern fixiert ist, lösen Sie die vorderen und hinteren Federn auf der Komponente.

c Wählen Sie zum Einsetzen der PCI-Karte einen Steckplatz auf der Riser-Karte der Komponente aus, und entfernen Sie die Blindplatte von diesem Slot.

Bei dem Modell WBG-5500-C müssen Sie den Riser-Slot 2 verwenden.

d Wenn die PCI-Karte mit einer Schraube fixiert ist, drehen Sie die Schraube heraus.

e Schieben Sie die PCI-Karte in den Slot hinein, bis sie beim Konnektor der Riser-Karte einrastet.

Schieben Sie die PCI-Karte behutsam ein, da der Konnektor bei übermäßigem Druck beschädigt werden könnte.

f Fixieren Sie die PCI-Karte mit der Schraube, oder schließen Sie die vorderen und hinteren Haltefedern.

g Bauen Sie die Komponente wieder ein.

4 Bringen Sie die Abdeckung der Appliance wieder an, und schließen Sie das Netzkabel an.

5 Schalten Sie die Appliance ein.

Weitere Informationen zur Installation finden Sie im *Intel Server System SR1625UR Service Guide (WBG-5000-B)* (Service-Handbuch für Intel Server System SR1625UR) bzw. *Intel Server System SR2600UR/SR2625UR Service Guide (WBG-5500-B)* (Service-Handbuch für Intel Server System SR2600UR/SR2625UR).

Diese Dokumente können Sie auf der Intel-Website herunterladen:

- http://download.intel.com/support/motherboards/server/s5520ur/sb/e52881005_sr1625ur_sg1.pdf (WBG-5000-B)
- http://download.intel.com/support/motherboards/server/s5520ur/sb/E51243-007_SR2600UR_SR2625UR_SG.pdf (WBG-5500-B)

4 Installation der Hardware-Verwaltungs-Tools

Beim Ausführen von Web Gateway auf einer physischen Appliance stehen Ihnen Tools zur Verfügung, mit denen Hardware-Verwaltungsaufgaben ausgeführt werden können. Sie können diese Tools nach dem Einrichten von Web Gateway installieren.

Inhalt

- *Tools für die Verwaltung der Web Gateway-Hardware*
- *Installieren des Plattformvertraulichkeitstest-Tools*
- *Ausführen eines Hardwaretests mit dem Plattformvertraulichkeitstest-Tool*
- *Konfigurieren des Remote Management Module*
- *Installieren der Active System Console*
- *Aktivieren des SNMP-Subagenten*

Tools für die Verwaltung der Web Gateway-Hardware

Für die Verwaltung der Hardware einer Web Gateway-Appliance stehen Ihnen mehrere Tools zur Verfügung.

Plattformvertraulichkeitstest-Tool

Mit dem PCT-Tool (Platform Confidence Test, Plattformvertraulichkeitstest) können Sie die Hardware-Funktionen einer Appliance testen. Während des Tests darf die Appliance nicht mit anderen Netzwerkgeräten verbunden sein.

Die Testergebnisse werden in der Datei *result.log* gespeichert, die Sie zur weiteren Verwendung auf ein USB-Laufwerk kopieren können.

Remote Management Module

Mit dem Remote Management Module (RMM) können Sie die Hardware-Funktionen einer Appliance per Remote-Zugriff verwalten.

Gemeinsam mit diesem Tool wird ein weiteres Tool installiert. Dabei handelt es sich um den Baseboard Management Controller (BMC). Dieses Tool muss ebenfalls ausgeführt werden, wenn Sie die Active System Console zum Abrufen von Debugging-Informationen verwenden möchten.

Die Schnittstelle für das Remote Management Module und den Baseboard Management Controller befindet sich an der Rückseite des Appliance-Gehäuses.

Active System Console

Die Active System Console (ASC) ist ein Web-basiertes Debugging-Tool. Es liefert Informationen über Hardware-Fehler im Zusammenhang mit dem Gehäuse, dem Speicher, den Lüftern, den Prozessoren, dem Arbeitsspeicher, der Stromversorgung sowie weiteren Komponenten.

Die Fehler werden vom Baseboard Management Controller erkannt, der zusammen mit dem Remote Management Module installiert wird. Der Baseboard Management Controller greift auf die Systemereignis- und Sensordatenaufzeichnungen auf einer Appliance zu.

Über die Active System Console können Sie die Einstellungen für den Baseboard Management Controller konfigurieren, beispielsweise seine IP-Adresse.

Mit dem Tool können Sie auch Hardware-bezogene Daten an McAfee senden.

SNMP-Subagent

Wenn SNMP-Überwachung (Simple Network Management Protocol) auf einer Appliance konfiguriert ist, können Sie mit dem SNMP-Subagent (SNMPSA) Hardware-bezogene Informationen abrufen, beispielsweise den CPU-Status, den Stromversorgungsstatus und aktuelle Sensorwerte.

Die SNMP-Informationen über den Status der Hardware-Komponenten wird in der Management Information Base (MIB) gespeichert.

Zur Bereitstellung der Informationen verwendet die Datenbank eine Verzeichnisstruktur von Objekten, die auf bestimmte Hardware-Komponenten und andere Elemente bezogen sind. Die Objekte werden mithilfe von Objekt-IDs (OIDs) identifiziert und aufgerufen.

Installieren des Plattformvertraulichkeitstest-Tools

Installieren Sie das PCT-Tool (Platform Confidence Test, Plattformvertraulichkeitstest), um Informationen zu Hardware-Fehlern abzurufen.

Für jedes Appliance-Modell ist eine spezielle Version des Tools vorhanden.

Vorgehensweise

1. Laden Sie die entsprechende Tool-Version über das McAfee Content & Cloud Security Portal herunter.

   Die Tool-Versionen stehen im ZIP-Format zur Verfügung.

2. Extrahieren Sie den Inhalt einer heruntergeladenen ZIP-Datei in das Stammverzeichnis eines USB-Laufwerks, das im Microsoft DOS-Modus formatiert ist.

3. Schließen Sie das USB-Laufwerk an die Appliance an.

4. Starten Sie die Appliance neu.

5. Drücken Sie bei einer entsprechenden Aufforderung **F2**, um das Einrichtungsmenü aufzurufen.

6. Wählen Sie **Server Management** | **Console Redirection** (Server-Verwaltung | Konsolenumleitung), und vergewissern Sie sich, dass **Console Redirection** (Konsolenumleitung) deaktiviert ist.

7. Wählen Sie **Boot Manager** (Boot-Manager), und klicken Sie auf **EFI Shell** (EFI-Shell).

   Die Appliance wird nun im EFI-Shell-Modus (Extensible Firmware Interface) neu gestartet.

Im EFI-Shell-Modus wird die Prozedur *startup.nsh* vom USB-Laufwerk ausgeführt, und ein Diagnosemenü wird angezeigt.

Sie können den Diagnosezyklus beenden, indem Sie **F10** drücken.

Ausführen eines Hardwaretests mit dem Plattformvertraulichkeitstest-Tool

Führen Sie zum Testen der Appliance-Hardware das PCT-Tool (Platform Confidence Test, Plattformvertraulichkeitstest) aus, und speichern Sie die Ergebnisse in einer Protokolldatei.

Bevor Sie beginnen

Vergewissern Sie sich, dass die Appliance mit keiner anderen Netzwerkkomponente verbunden ist.

Vorgehensweise

1 Wählen Sie im Diagnosemenü des Tools einen Testtyp aus.

Beim Testen der Netzwerkschnittstellen-Anschlüsse können Sie jeden gewünschten Anschluss über ein Crossover-Kabel mit einem beliebigen Anschluss im gleichen System verbinden.

Der Test wird ausgeführt, und das Ergebnis wird in eine Protokolldatei auf einem RAM-Datenträger geschrieben. Der Name der Protokolldatei lautet *result.log*.

2 Kopieren Sie die Datei *result.log* auf das USB-Laufwerk.

a Führen Sie den Befehl *map* aus.

b Ermitteln Sie das USB-Laufwerk in der angezeigten Liste. Geben Sie anschließend den folgenden Befehl ein:

`cp result.log blk0:` <Name des USB-Laufwerks>

In diesem Befehl steht *blk0* für einen Geräteparameter, der bei Verwendung eines USB-Laufwerks erforderlich ist.

In einigen Fällen können an dieser Stelle andere Geräteparameter angegeben werden.

Es empfiehlt sich, das System nach der Durchführung eines umfassenden Tests oder Looping-Tests vollständig durchzustarten (d. h. aus- und dann wieder einzuschalten), bevor Sie es nach dem Test wieder anderweitig nutzen.

Dadurch werden alle Controller zurückgesetzt, sodass sie dann zuverlässig im erwarteten Modus ausgeführt werden.

Konfigurieren des Remote Management Module

Wenn Sie das Remote Management Module (RMM) konfigurieren, können Sie die Appliance-Hardware per Remote-Zugriff verwalten.

Bei der Installation können Sie auch das Unterstützungs-Tool Baseboard Management Controller (BMC) installieren.

Vorgehensweise

1 Verbinden Sie die Schnittstellen für das Remote Management Module und/oder den Baseboard Management Controller an der Rückseite des Appliance-Gehäuses mit dem Netzwerk.

2 Starten Sie die Appliance neu.

3 Drücken Sie während der Startphase **F2**.

Daraufhin öffnet sich ein Konfigurationsmenü.

4 Wählen Sie **Server Management** | **BMC LAN Configuration**(Server-Verwaltung | BMC-LAN-Konfiguration) aus.

5 Konfigurieren Sie unter **Baseboard LAN configuration** (Baseboard-LAN-Konfiguration) eine IP-Adresse, eine Subnetzmaske und eine Gateway-IP-Adresse.

6 Konfigurieren Sie unter **Intel (R) RMM3 LAN configuration** (Intel (R) RMM3-LAN-Konfiguration) oder **Intel (R) RMM4 LAN configuration** (Intel (R) RMM4-LAN-Konfiguration) (für WBG-xxxx-C-Modelle) eine IP-Adresse, eine Subnetzmaske und eine Gateway-IP-Adresse.

7 Konfigurieren Sie unter **User configuration** (Benutzerkonfiguration) einen Benutzernamen und ein Kennwort, damit ein Erstbenutzer das Remote Management Module aufrufen kann.

8 Drücken Sie **F10**, und klicken Sie im daraufhin geöffneten Dialogfeld auf **Yes** (Ja), um Ihre Einstellungen zu speichern.

Nun können Sie mit dem Remote Management Module die Appliance-Hardware per Remote-Zugriff verwalten. Das Modul rufen Sie über die konfigurierte IP-Adresse auf.

Die Schnittstelle für das Remote Management Module und den Baseboard Management Controller befindet sich zwischen den Netzwerkschnittstellen an der Rückseite des Appliance-Gehäuses. Eine schematische Darstellung der Position der Schnittstellen finden Sie im Abschnitt *Port-Zuweisungen* des Kapitels *Einrichtung von Web Gateway* im vorliegenden Handbuch.

Installieren der Active System Console

Installieren Sie die Active System Console (ASC), um Debugging-Informationen zur Appliance-Hardware abzurufen.

Hardware-Informationen können Sie über die Active System Console oder über den SNMP-Subagenten abrufen.

Vorgehensweise

1 Melden Sie sich von einer Systemkonsole über SSH bei der Appliance an. Führen Sie dabei den folgenden Befehl aus:

```
asc-enable
```

2 Führen Sie den folgenden Befehl aus:

```
asc-enable
```

3 Erstellen Sie bei einer entsprechenden Aufforderung ein Administratorkennwort.

Wenn eine Meldung mit bestimmten Anforderungen für das Kennwort angezeigt wird, legen Sie ein Kennwort fest, dass diesen Vorgaben entspricht.

Nach dem Festlegen des Kennworts wird die Active System Console gestartet.

4 Greifen Sie in einem Web-Browser unter folgender Adresse auf die ASC-Benutzeroberfläche zu:

`https://`<IP-Adresse der überwachten Appliance>`:9393`

Beim nächsten Start der Appliance wird diese automatisch zusammen mit der Active System Console gestartet.

Sie können die Active System Console mithilfe des Befehls *asc-disable* deaktivieren.

Weitere Informationen hierzu finden Sie in der Hilfe zur Benutzeroberfläche der Active System Console sowie in der Dokumentation, die mit der Hardware bereitgestellt wird.

Aktivieren des SNMP-Subagenten

Aktivieren Sie den SNMP-Subagenten (SNMPSA) von einer Systemkonsole, um Informationen zum Hardware-Status einer Appliance abzurufen.

Hardwareinformationen können Sie entweder über den SNMP-Subagenten oder die Active System Console abrufen.

Vorgehensweise

1. Vergewissern Sie sich, dass die SNMP-Einstellungen auf der Benutzeroberfläche der Appliance konfiguriert sind.

   Weitere Informationen zum Konfigurieren dieser Einstellungen finden Sie im Kapitel *Überwachung* des *Produkthandbuchs zu McAfee Web Gateway*.

2. Melden Sie sich von einer Systemkonsole mithilfe von SSH bei der Appliance an.

3. Führen Sie den folgenden Befehl aus:

   ```
   snmpsa-enable
   ```

   Daraufhin wird der SNMP-Subagent aktiviert.

   Sie können den SNMP-Subagenten mit dem Befehl `snmpsa-disable` deaktivieren.

Wenn der SNMP-Subagent aktiviert ist, sind unter dem SNMP-Protokoll Daten zum Hardware-Status verfügbar.

Einen Überblick über diese verfügbaren Informationen finden Sie in den MIB-Dateien (Management Information Base), die sich im Dateisystem der überwachten Appliance befinden. Der Pfad zu diesen Dateien lautet */usr/local/snmpsa/mibs*.

Weitere Informationen zum Arbeiten mit dem SNMP-Subagenten finden Sie im *Intel SNMP Subagent User Guide* (Benutzerhandbuch zum SNMP-Subagenten).

Sie können dieses Dokument von der Intel-Website unter der Adresse http://www.intel.com/support/motherboards/server/sysmgmt/sb/CS-029304.htm herunterladen.

5 Installation von Web Gateway auf einem Blade-Server

Sie können einen Blade-Server in einem Blade-System-Gehäuse als Hardware-Plattform für Web Gateway verwenden.

Inhalt

- *Unterstützte Blade-Server und Gehäuse*
- *Installation des Blade-Server-Systems*
- *Netzwerkeinrichtung von Web Gateway auf einem Blade-Server*
- *Anschlusszuweisungen auf einem Blade-Server*

Unterstützte Blade-Server und Gehäuse

Ein Blade-Server ist ein modularer Server, der in einem Blade-System-Gehäuse installiert ist.

Die für die Verwendung mit Web Gateway bereitgestellten Blade-Server-Modelle werden auch als *McAfee-Blades* bezeichnet.

Web Gateway kann auf den folgenden Blade-Server-Modellen ausgeführt werden:

- ProLiant BL460c G6
- ProLiant BL460c G6.5
- ProLiant BL460C G8

Die Blade-Server können in den folgenden Gehäusemodellen installiert werden:

- M3 (c3000)
- M7 (c7000)

Installation des Blade-Server-Systems

Wenn Sie Web Gateway auf einem Blade-Server ausführen möchten, müssen Sie das Blade-System-Gehäuse mit den Blade-Servern installieren.

Ein Blade-System-Gehäuse mit darin installierten Blade-Servern wird als *Blade-Server-System* bezeichnet.

Ein ausführliche Beschreibung der Installation eines Blade-Server-Systems finden Sie in der Dokumentation des McAfee Partners (Hewlett-Packard), der Blade-Server für Web Gateway bereitstellt. Die Dokumentation ist auf der Website von Hewlett-Packard verfügbar.

Vorbereiten der Installation des Blade-Server-Systems

Beim Installieren eines Blade-Server-Systems müssen verschiedene Voraussetzungen erfüllt sein.

Beim Vorbereiten der Installation sind die im Folgenden beschriebenen Aspekte zu berücksichtigen.

Umgebung des Blade-Server-Systems

Sie müssen die Umgebung des Blade-Server-Systems berücksichtigen.

- Stromversorgung und Klimatisierung
- Integration des Blade-Server-Systems in Ihr Netzwerk

Vollständigkeit der Lieferung

Sie müssen anhand des Lieferscheins genau überprüfen, ob Sie alle zugehörigen Komponenten erhalten haben.

- Blade-Server-Gehäuse (M3 oder M7) mit Blade-Servern
- Netzkabel
- Netzwerkkabel

IP-Adressen für das Blade-Server-System

Im Blade-Server-System sind IP-Adressen für folgende Komponenten erforderlich:

- Onboard-Administrator-Modul
- iLO-Module (integrated Lights Out) – 8 bis 16 Adressen (je nach Konfiguration)
- Interconnect-Module – 4 Adressen
- Blade-Server (die Anzahl der Adressen hängt von der jeweiligen Konfiguration ab)

Ausführliche Informationen hierzu finden Sie im *Site Planning Guide* (Handbuch zur Standortplanung) und im *Setup and Installation Guide* (Einrichtungs- und Installationshandbuch), das für die einzelnen Gehäusemodelle auf der Website des McAfee Partners verfügbar ist.

Installieren des Blade-Server-Systems

Installieren Sie zum Installieren des Blade-Server-Systems zunächst das Gehäuse des Blade-Systems, setzen Sie die Interconnect-Module in das Gehäuse ein, und schalten Sie das Gehäuse dann ein.

Aufgaben

- *Installieren des Blade-System-Gehäuses* auf Seite 45
  Entnehmen Sie das Blade-System-Gehäuse zum Installieren zunächst aus der Verpackung, installieren Sie die einzelnen Komponenten, und schließen Sie einen Monitor und eine Tastatur an.
- *Installieren der Interconnect-Module* auf Seite 45
  Setzen Sie die Interconnect-Module zum Installieren in die Interconnect-Modul-Einschübe im Blade-System-Gehäuse ein.
- *Einschalten des Blade-System-Gehäuses* auf Seite 46
  Schließen Sie das Blade-System-Gehäuse an die Stromversorgung an, und schalten Sie es ein.
- *Installieren von Web Gateway auf einem Blade-Server* auf Seite 46
  Laden Sie zum Installieren von Web Gateway auf einem Blade-Server die Appliance-Software herunter, wählen Sie ein Installationsmedium und einen Blade-Server aus, und führen Sie den Installationsvorgang aus.

Installieren des Blade-System-Gehäuses

Entnehmen Sie das Blade-System-Gehäuse zum Installieren zunächst aus der Verpackung, installieren Sie die einzelnen Komponenten, und schließen Sie einen Monitor und eine Tastatur an.

Vorgehensweise

1 Lesen Sie die beiliegenden Sicherheitsvorschriften aufmerksam durch, und befolgen Sie sie.

2 Nehmen Sie das Produkt aus der Schutzverpackung, und stellen Sie das Blade-System-Gehäuse auf eine ebene Fläche.

Packen Sie in Anbetracht des Gewichts des Gehäuses dieses so nahe wie möglich am gewünschten Standort aus.

3 Entfernen Sie die vorderen und hinteren Elemente sowie den hinteren Käfig vom Gehäuse.

4 Bringen Sie die Netzteile und die Lüfter an.

Es wird empfohlen, alle im Lieferumfang des Gehäuses enthaltenen Netzteile und Lüfter anzubringen, um die Redundanz bei Ausfall einer dieser Komponenten sicherzustellen.

5 Installieren Sie das Onboard-Administrator-Modul sowie das iLO-System (integrated Lights Out).

6 Schließen Sie einen Bildschirm und eine Tastatur an das Gehäuse an.

7 Schließen Sie Netzkabel an den Monitor und das Gehäuse an, schließen Sie die Netzteile jedoch vorerst noch nicht an.

Weitere Informationen hierzu finden Sie im *Setup and Installation Guide* (Setup- und Installationshandbuch), im *Onboard Administrator User Guide* (Onboard-Administrator-Benutzerhandbuch) und im *Integrated Lights-Out User Guide* (iLO-Benutzerhandbuch), die auf der Website des McAfee Partners für die einzelnen Gehäusemodelle verfügbar sind.

Installieren der Interconnect-Module

Setzen Sie die Interconnect-Module zum Installieren in die Interconnect-Modul-Einschübe im Blade-System-Gehäuse ein.

Über das Onboard-Administrator-Modul des Gehäuses können Sie ein Diagramm des Gehäuses einsehen. Führen Sie den Mauszeiger über das Diagramm, um die Lage der Interconnect-Modul-Einschübe an der Gehäuserückseite zu ermitteln.

Das M3-Gehäuse enthält vier Interconnect-Modul-Einschübe, während das M7-Gehäuse mit acht Einschüben ausgestattet ist. Bei diesen Modulen handelt es sich entweder um Durchgangsmodule oder Switches.

Vorgehensweise

1 Ermitteln Sie die Lage der Interconnect-Modul-Einschübe.

2 Installieren Sie Interconnect-Module wie im Folgenden beschrieben.

- Wenn Sie über ein M3-Gehäuse verfügen, setzen Sie vier Switches in die Interconnect-Modul-Einschübe 1 bis 4 ein.
- Wenn Sie über ein M7-Gehäuse verfügen, setzen Sie vier Switches in die Interconnect-Modul-Einschübe 1 bis 4 und zwei Durchgangsmodule in die Interconnect-Modul-Einschübe 5 und 6 ein.

Einschalten des Blade-System-Gehäuses

Schließen Sie das Blade-System-Gehäuse an die Stromversorgung an, und schalten Sie es ein.

Vorgehensweise

1 Schließen Sie die Netzkabel des Gehäuses an die Stromversorgung und die Netzbuchsen an.

Es empfiehlt sich, zwei Stromkreise zu verwenden, um sicherzustellen, dass alle Blade-Server im Gehäuse eingeschaltet werden.

Wenn Sie nur einen Stromkreis verwenden und die Energieverwaltungseinstellungen auf den redundanten Wechselstrommodus festgelegt sind (dies wird empfohlen), können einige Blade-Server nicht eingeschaltet werden.

2 Schalten Sie das Blade-System-Gehäuse ein.

Sie können nun die Web Gateway-Appliance-Software auf einem Blade-Server im Gehäuse installieren.

Installieren von Web Gateway auf einem Blade-Server

Laden Sie zum Installieren von Web Gateway auf einem Blade-Server die Appliance-Software herunter, wählen Sie ein Installationsmedium und einen Blade-Server aus, und führen Sie den Installationsvorgang aus.

Sie können die Web Gateway-Appliance-Software im ISO- oder USB-Format über das McAfee Content & Cloud Security Portal unter https://contentsecurity.mcafee.com/software_mwg7_download herunterladen.

Sie können verschiedene Medien zum Installieren von Web Gateway auf einem Blade-Server nutzen. Dies hängt vom Gehäusemodell ab:

- Internes CD/DVD-Laufwerk: M3
- Externes CD/DVD-Laufwerk: M7
- USB-Laufwerk: M3 und M7
- Virtuelles Medium: M3 und M7

Nachdem Sie ein Installationsmedium ausgewählt haben, müssen Sie einen der folgenden Tasks ausführen.

Aufgaben

- *Installieren von Web Gateway auf einem Blade-Server über ein internes CD/DVD-Laufwerk* auf Seite 47
  Wenn Sie über ein M3-Gehäuse verfügen, können Sie die Web Gateway-Appliance-Software auf einem Blade-Server im Gehäuse über das interne CD/DVD-Laufwerk installieren.
- *Installieren von Web Gateway auf einem Blade-Server über ein externes CD/DVD-Laufwerk* auf Seite 48
  Wenn Sie über ein M7-Gehäuse verfügen, können Sie die Web Gateway-Appliance-Software auf einem Blade-Server im Gehäuse über ein externes CD/DVD-Laufwerk installieren.
- *Installieren von Web Gateway auf einem Blade-Server anhand eines USB-Laufwerks* auf Seite 48
  Sie können die Web Gateway-Appliance-Software auf einem Blade-Server in beiden Gehäusemodellen mithilfe eines USB-Laufwerks installieren.
- *Verwenden von virtuellen Medien zum Installieren von Web Gateway auf einem Blade-Server* auf Seite 48
  Zum Installieren der Web Gateway-Appliance-Software auf einem Blade-Server können Sie bei beiden Gehäusemodellen ein virtuelles Medium verwenden. Das Blade-Systemgehäuse bietet eine Option für die virtuelle Installation von McAfee Web Gateway auf einem Server im Gehäuse mithilfe eines ISO-Images, das auf einem lokalen Laufwerk gespeichert ist.

Installieren von Web Gateway auf einem Blade-Server über ein internes CD/DVD-Laufwerk

Wenn Sie über ein M3-Gehäuse verfügen, können Sie die Web Gateway-Appliance-Software auf einem Blade-Server im Gehäuse über das interne CD/DVD-Laufwerk installieren.

Vorgehensweise

1. Legen Sie eine CD oder DVD mit der Web Gateway-Appliance-Software in das interne CD/DVD-Laufwerk des Gehäuses ein.
2. Öffnen Sie den Onboard-Administrator des Gehäuses, und wählen Sie den Blade-Server aus, auf dem Sie Web Gateway installieren möchten.
3. Klicken Sie auf die Registerkarte **Virtual Devices** (Virtuelle Geräte).
4. Stellen Sie mithilfe dieser Registerkarte eine Verbindung des internen CD/DVD-Laufwerks mit dem Blade-Server her.
5. Klicken Sie auf die Registerkarte **Boot Options** (Startoptionen), und wählen Sie für **One Time Boot from** (Einmaliges Starten von) **CD-ROM** aus.
6. Schalten Sie den Blade-Server ein.
7. Befolgen Sie die Anweisungen zur Installation von Web Gateway, die auf dem Monitor angezeigt werden, den Sie an das Gehäuse angeschlossen haben.

Nach Abschluss der Installation können Sie sich bei der Benutzeroberfläche von Web Gateway anmelden.

Weitere Informationen zum Anmelden und den darauf folgenden Schritten finden Sie im Kapitel *Einrichtung von Web Gateway* dieses Handbuchs.

Installieren von Web Gateway auf einem Blade-Server über ein externes CD/DVD-Laufwerk

Wenn Sie über ein M7-Gehäuse verfügen, können Sie die Web Gateway-Appliance-Software auf einem Blade-Server im Gehäuse über ein externes CD/DVD-Laufwerk installieren.

Vorgehensweise

1. Legen Sie eine CD oder DVD mit der Web Gateway-Appliance-Software in das externe CD/DVD-Laufwerk ein.
2. Verbinden Sie mit dem im Lieferumfang des Gehäuses enthaltenen USB-SUV-Kabel das Laufwerk mit dem Blade-Server, auf dem Web Gateway installiert werden soll.
3. Öffnen Sie das Onboard-Administrator-Modul des Gehäuses, und wählen Sie den Blade-Server aus.
4. Klicken Sie auf die Registerkarte **Boot Options** (Startoptionen), und wählen Sie für **One Time Boot from** (Einmaliges Starten von) **CD-ROM** aus.
5. Schalten Sie den Blade-Server ein.
6. Befolgen Sie die Anweisungen zur Installation von Web Gateway, die auf dem Monitor angezeigt werden, den Sie an das Gehäuse angeschlossen haben.

Nach Abschluss der Installation können Sie sich bei der Benutzeroberfläche von Web Gateway anmelden.

Weitere Informationen zum Anmelden und den darauf folgenden Schritten finden Sie im Kapitel *Einrichtung von Web Gateway* dieses Handbuchs.

Installieren von Web Gateway auf einem Blade-Server anhand eines USB-Laufwerks

Sie können die Web Gateway-Appliance-Software auf einem Blade-Server in beiden Gehäusemodellen mithilfe eines USB-Laufwerks installieren.

Vorgehensweise

1. Verbinden Sie mit dem im Lieferumfang des Gehäuses enthaltenen USB-SUV-Kabel das USB-Laufwerk mit dem Blade-Server, auf dem Web Gateway installiert werden soll.
2. Öffnen Sie das Onboard-Administrator-Modul des Gehäuses, und wählen Sie den Blade-Server aus.
3. Klicken Sie auf die Registerkarte **Virtual Devices** (Virtuelle Geräte).
4. Klicken Sie auf die Registerkarte **Boot Options** (Startoptionen), und wählen Sie für **One Time Boot from** (Einmaliges Starten von) **USB** aus.
5. Schalten Sie den Blade-Server ein.
6. Befolgen Sie die Anweisungen zur Installation von Web Gateway, die auf dem Monitor angezeigt werden, den Sie an das Gehäuse angeschlossen haben.

Nach Abschluss der Installation können Sie sich bei der Benutzeroberfläche von Web Gateway anmelden.

Weitere Informationen zum Anmelden und den darauf folgenden Schritten finden Sie im Kapitel *Einrichtung von Web Gateway* dieses Handbuchs.

Verwenden von virtuellen Medien zum Installieren von Web Gateway auf einem Blade-Server

Zum Installieren der Web Gateway-Appliance-Software auf einem Blade-Server können Sie bei beiden Gehäusemodellen ein virtuelles Medium verwenden. Das Blade-Systemgehäuse bietet eine Option für

die virtuelle Installation von McAfee Web Gateway auf einem Server im Gehäuse mithilfe eines ISO-Images, das auf einem lokalen Laufwerk gespeichert ist.

Das Blade-Systemgehäuse bietet eine Option für die virtuelle Installation von Web Gateway auf einem Server im Gehäuse mithilfe eines ISO-Images, das auf einem lokalen Laufwerk gespeichert ist.

Vorgehensweise

1. Öffnen Sie den Onboard-Administrator des Gehäuses, und wählen Sie den Blade-Server aus, auf dem Sie Web Gateway installieren möchten.
2. Klicken Sie auf **iLO** und dann auf **Web Administration** (Web-Verwaltung).

   Daraufhin öffnet sich ein neues Browser-Fenster, in dem Sie auf die Web-Benutzerschnittstelle von iLO (integrated Lights-Out) zugreifen können.
3. Klicken Sie auf die Registerkarte **Virtual Media** (Virtuelles Medium) und dann auf **Virtual Media** (Virtuelles Medium).

   Daraufhin öffnet sich das Fenster **Virtual Media** (Virtuelles Medium).
4. Wählen Sie im Fenster für die Installation von Web Gateway die Option **Virtual Floppy/USB Key** (Virtuelle Diskette/Virtueller USB-Stick) oder **Virtual CD/DVD-ROM** (Virtuelle CD/DVD), und klicken Sie dann auf **Browse** (Durchsuchen).
5. Navigieren Sie zum Speicherort des ISO-Images der Web Gateway-Appliance-Software, und klicken Sie auf **Connect** (Verbinden).

   Das ISO-Image steht nun zur Installation zur Verfügung.
6. Befolgen Sie die Anweisungen zur Installation von Web Gateway, die auf dem Monitor angezeigt werden, den Sie an das Gehäuse angeschlossen haben.

Nach Abschluss der Installation können Sie sich bei der Benutzeroberfläche von Web Gateway anmelden.

Informationen zur Anmeldung und weiteren Vorgehensweise finden Sie im Kapitel *Einrichtung von Web Gateway* dieses Handbuchs.

Netzwerkeinrichtung von Web Gateway auf einem Blade-Server

Nach dem Installieren von McAfee Web Gateway auf einem McAfee Blade-Server können Sie die Netzwerkeinrichtung konfigurieren.

Sie können eine der folgenden Einrichtungen konfigurieren:

- Proxy-Hochverfügbarkeit
- Proxy mit externem Lastenausgleich
- Transparenter Router
- Transparente Bridge

Für jede dieser Einrichtungen müssen Sie die entsprechenden Einstellungen in der Benutzeroberfläche von McAfee Web Gateway konfigurieren und zusätzliche Konfigurationsschritte für die übrigen Netzwerkkomponenten ausführen.

Proxy-Hochverfügbarkeit auf einem Blade-Server

Sie können den Proxy HA-Modus (High Availability, Hochverfügbarkeit) für Web Gateway auf einem Blade-Server konfigurieren. Dieser Modus bietet die Funktionen eines Proxys, der als explizierter Proxy ausgeführt wird, in Kombination mit Hochverfügbarkeitsfunktionen.

Netzwerkkonfiguration

Für diese Hochverfügbarkeitskonfiguration müssen mehrere Instanzen von Web Gateway auf Blade-Servern vorhanden sein, die in dieser Konfiguration als Knoten ausgeführt werden. Es muss mindestens zwei Master-Knoten geben, sodass bei Ausfall eines Knotens ein Failover durchgeführt werden kann. Ein Master-Knoten leitet Datenpakete an die Knoten weiter, die die Daten so scannen, dass ein Lastausgleich möglich ist.

Es wird empfohlen, den Proxy-Hochverfügbarkeitsmodus als *zweigleisige Proxy-Lösung* zu konfigurieren. Das bedeutet, dass Folgendes auf einem Master-Knoten konfiguriert wird:

- Netzwerkschnittstelle für eingehenden Web-Datenverkehr
- Netzwerkschnittstelle für ausgehenden Web-Datenverkehr

Die Netzwerkschnittstelle für den eingehenden Datenverkehr muss eine eigene virtuelle IP-Adresse besitzen. Die Netzwerkschnittstelle für ausgehenden Web-Datenverkehr sollte auch für den Lastausgleich verwendet werden. Das erreichen Sie, indem Sie deren IP-Adresse als physische Komponente angeben, die zusammen mit der Verwaltungs-IP-Adresse konfiguriert wird.

Außerdem werden folgende Konfigurationen auf jedem Master-Knoten empfohlen:

- Netzwerkschnittstelle für Out of Band-Verwaltung

  Wenn Sie diese Netzwerkschnittstelle konfigurieren, kann die Verwaltungskommunikation separat durchgeführt werden.

- Netzwerkschnittstelle für interne Kommunikation innerhalb des Blade-Systemgehäuses

  Die IP-Adresse dieser Netzwerkschnittstelle wird unter VRRP (Virtual Router Redundancy Protocol) konfiguriert.

Beständigkeit der Verbindung

Wenn Switches als Interconnect-Module auf einem Gehäuse installiert werden, können Sie die Beständigkeit der Verbindung wie folgt erreichen:

- Zwei der als *Uplink-Anschlüsse* genutzten Anschlüsse auf einem Switch werden in einer Trunk-Gruppe gebündelt.
- Jeder dieser beiden Anschlüsse ist über ein Netzwerkkabel mit einer physischen Verbindung verbunden.

Dadurch bleibt die Trunk-Gruppe aktiv, auch wenn eine der beiden Verbindungen ausfällt.

Die Interconnect-Module und die Trunk-Gruppen werden den Anschlüssen an den Netzwerkschnittstellen zugeordnet, beispielsweise wie in der folgenden Tabelle. Für die Netzwerkschnittstelle, die für die interne Kommunikation zuständig ist, muss kein Anschluss einer Trunk-Gruppe zugeordnet werden.

Tabelle 5-1 Zuordnung der Netzwerkkomponenten in einer Proxy-Hochverfügbarkeitskonfiguration

Anschluss auf Netzwerkschnittstelle	Interconnect-Modul	Trunk-Gruppe
Schnittstelle für eingehenden Web-Datenverkehr	Switch in Interconnect-Modul-Einschub 1	Gruppe 1: Anschluss 21, Anschluss 22
Schnittstelle für ausgehenden Web-Datenverkehr	Switch in Interconnect-Modul-Einschub 2	Gruppe 2: Anschluss 21, Anschluss 22
Schnittstelle für die Out of Band-Verwaltung	Switch in Interconnect-Modul-Einschub 3	Gruppe 3: Anschluss 21, Anschluss 22
Schnittstelle für die interne Kommunikation	Switch in Interconnect-Modul-Einschub 4	keine Uplink-Anschlüsse erforderlich

Weitere Informationen zur Konfiguration der Interconnect-Module finden Sie im Anwendungshandbuch *GbE2c Ethernet Blade Switch for c-Class BladeSystem Application Guide*, das auf der Website des McAfee-Partners verfügbar ist.

Proxy mit externem Lastausgleich auf einem Blade-Server

Auf einem Blade-Server, bei dem der Lastausgleich von einem externen Gerät durchgeführt wird, können Sie den expliziten Modus für Web Gateway konfigurieren.

Netzwerkkonfiguration

Es wird empfohlen, eine *zweigleisige Proxy-Lösung* für diesen Modus zu konfigurieren, mit zwei separaten Netzwerkschnittstellen für eingehenden und ausgehenden Web-Datenverkehr auf jedem Blade-Server. Jede dieser Schnittstellen wird mit einer eigenen IP-Adresse konfiguriert.

Außerdem sollten Sie zusätzlich eine Netzwerkschnittstelle für Out of Band-Verwaltung konfigurieren, sodass auch der Verwaltungsdatenverkehr separat durchgeführt werden kann.

Lastausgleich

Der Lastausgleich wird in dieser Konfiguration nicht von einem der Blade-Server durchgeführt, sondern von einem externen Lastausgleichsgerät, das die Last an die Blade-Server weiterleitet. Zu diesem Zweck sind die Blade-Server in einen Lastausgleichs-Pool integriert.

Bei der Konfiguration des Lastausgleichsgeräts können Sie einen Algorithmus konfigurieren, der die IP-Client-Bindung unterstützt. So können Funktionen bereitgestellt werden, die IP-Client-Bindung erfordern, beispielsweise eine Fortschrittsseite.

Beständigkeit der Verbindung

Wenn Switches als Interconnect-Module auf einem Gehäuse installiert werden, können Sie die Beständigkeit der Verbindung wie folgt erreichen:

- Zwei der als *Uplink-Anschlüsse* genutzten Anschlüsse auf einem Switch werden in einer Trunk-Gruppe gebündelt.
- Jeder dieser beiden Anschlüsse ist über ein Netzwerkkabel mit einer physischen Verbindung verbunden.

Dadurch bleibt die Trunk-Gruppe aktiv, auch wenn eine der beiden Verbindungen ausfällt.

Die Interconnect-Module und die Trunk-Gruppen werden den Anschlüssen an den Netzwerkschnittstellen zugeordnet, beispielsweise wie in der folgenden Tabelle.

Tabelle 5-2 Zuordnung der Netzwerkkomponenten in einer Konfiguration für einen expliziten Proxy mit externem Lastausgleich

Anschluss auf Netzwerkschnittstelle	Interconnect-Modul	Trunk-Gruppe
Schnittstelle für eingehenden Web-Datenverkehr	Switch in Interconnect-Modul-Einschub 1	Gruppe 1: Anschluss 21, Anschluss 22
Schnittstelle für ausgehenden Web-Datenverkehr	Switch in Interconnect-Modul-Einschub 2	Gruppe 2: Anschluss 21, Anschluss 22
Schnittstelle für die Out of Band-Verwaltung	Switch in Interconnect-Modul-Einschub 3	Gruppe 3: Anschluss 21, Anschluss 22

Weitere Informationen zur Konfiguration der Interconnect-Module finden Sie im Anwendungshandbuch *GbE2c Ethernet Blade Switch for c-Class BladeSystem Application Guide*, das auf der Website des McAfee-Partners verfügbar ist.

Transparente Modi auf einem Blade-Server

Sie können transparente Modi für Web Gateway auf einem Blade-Server konfigurieren.

In diesen Modi wird Web Gateway als transparenter Router ausgeführt, der Datenpakete zwischen den verschiedenen Segmenten Ihres Netzwerks weiterleitet oder als transparente Bridge fungiert, die das Weiterleiten von Datenpaketen zwischen diesen Segmenten ermöglicht.

Transparenter Router

Es wird empfohlen, für diesen Modus eine *zweigleisige Proxy-Lösung* mit zwei separaten Netzwerkschnittstellen für eingehenden und ausgehenden Web-Datenverkehr zu konfigurieren.

Jede dieser Netzwerkschnittstellen wird mit ihrer eigenen IP-Adresse unter VRRP (Virtual Router Redundancy Protocol) konfiguriert.

Die ausgehende Netzwerkschnittstelle sollte dabei für den Lastausgleich des Datenverkehrs verwendet werden. Das erreichen Sie, indem Sie deren IP-Adresse als physische Komponente angeben, die zusammen mit der Verwaltungs-IP-Adresse konfiguriert wird.

Wenn IP-Spoofing konfiguriert ist, benötigen die Blade-Server, auf denen Web Gateway nur den Web-Datenverkehr scannt, ohne ihn in bestimmte Richtungen zu leiten, keine Verbindung für eingehenden Web-Datenverkehr. Der ein- und ausgehende Datenverkehr wird von einer Web Gateway-Instanz verwaltet, die als Master-Knoten auf einem Blade-Server ausgeführt wird.

Transparente Bridge

Es wird empfohlen, auch für diesen Modus eine *zweigleisige Proxy-Lösung* mit zwei separaten Netzwerkschnittstellen für eingehenden und ausgehenden Web-Datenverkehr zu konfigurieren.

Für diesen Netzwerkmodus benötigt die zweigleisige Lösung keine virtuellen IP-Adressen und dementsprechend erfolgt auch keine Kommunikation unter VRRP.

Wenn Sie die Verwaltungs-IP-Adresse konfigurieren, müssen Sie die IP-Adresse der Netzwerkschnittstelle angeben, die als Bridge-Schnittstelle *ibr0* konfiguriert wurde.

Dem Master-Knoten für den Lastausgleich wird diese Rolle gemäß STP (Spanning Tree Protocol) zugewiesen.

Sie müssen die STP-Verwendung an Switches im Gehäuse für ein- und ausgehenden Web-Datenverkehr deaktivieren, um sicherzustellen, dass der Master-Knoten ordnungsgemäß unter STP zugewiesen wird. STP wird dann vom Betriebssystem ausgeführt.

Wenn die Lastausgleichsrolle auf einem Master-Knoten unter STP zugewiesen wurde, muss dieses Protokoll an den Switches deaktiviert werden, und zwar nicht nur, wenn Web Gateway auf einem Blade-Server ausgeführt wird, sondern auch, wenn es auf einer Appliance-Box oder einer virtuellen Maschine ausgeführt wird.

Anschlusszuweisungen auf einem Blade-Server

Bei der Ausführung auf einem Blade-Server verwendet Web Gateway die Netzwerkschnittstellen des betreffenden Blade-Servers. Die Anschlüsse, die diesen Netzwerkschnittstellen zugewiesen sind, werden von den Interconnect-Modulen in einem Gehäuse physisch bereitgestellt.

Die Netzwerkschnittstellen eines Blade-Servers befinden sich auf seiner Systemplatine und auf zusätzlichen Netzwerkschnittstellenkarten (so genannten Tochterkarten). Die Interconnect-Module, die die Anschlüsse für die Netzwerkschnittstellen bereitstellen, befinden sich in den Interconnect-Modul-Einschüben eines Gehäuses.

Anschlüsse können Netzwerkschnittstellen zugewiesen werden, es können jedoch auch die Beziehungen zwischen allen an der Kommunikation in einem Blade-Server-System beteiligten Komponenten zugewiesen werden.

Die Zuordnung der Komponenten in einem Blade-Server-System kann im Onboard-Administrator-Modul des Gehäuses angezeigt werden.

Interconnect-Module und Einschübe

Interconnect-Module in einem Blade-Server-System, in dem Web Gateway ausgeführt werden kann, können Folgendes sein:

- Durchgangsmodule (HP 1Gb Ethernet-Pass-Thru-Module)
- Switches (HP GbE2c Layer 2/3 Ethernet Blade-Switches, auch als LAN-Interconnects bezeichnet)

Ein Interconnect-Modul kann 16 Anschlüsse (Durchgangsmodul) bzw. fünf Anschlüsse (Switch) physisch bereitstellen. Ein M3-Gehäuse weist vier Interconnect-Modul-Einschübe auf, während ein M7-Modell mit acht Einschüben ausgestattet ist. Ein Blade-Server-System kann also zwischen 20 und 128 Anschlüsse enthalten.

Netzwerkschnittstelle und Karten

In die Systemplatine können bis zu acht Netzwerkschnittstellen integriert sein, und es können zwei zusätzliche Karten (Tochterkarten) vorhanden sein:

- Zwei LoM (LAN on Motherboard)-Netzwerkschnittstellen in die Systemplatine integriert
- Zwei Netzwerkschnittstellen auf Tochterkarte 1
- Vier Netzwerkschnittstellen auf Tochterkarte 2

Ein Gehäuse kann bis zu 16 Blade-Server enthalten. Ein Blade-Server-System kann also zwischen zwei (nur ein Blade-Server mit der Systemplatinenkarte in einem Gehäuse) und 128 Netzwerkschnittstellen enthalten.

Die Anzahl der Anschlüsse und die Anzahl der Netzwerkschnittstellen können daher übereinstimmen bzw. mehr oder minder stark voneinander abweichen. Es kann ein Anschluss für jede Netzwerkschnittstelle vorhanden sein, die Anzahl der Anschlüsse kann die Anzahl der Netzwerkschnittstellen jedoch auch über- bzw. unterschreiten.

Zuordnen von Netzwerkschnittstellen, Abschlüssen und Interconnect-Modul-Einschüben

Die Anschlüsse für die Netzwerkschnittstellen auf einem Blade-Server werden den Interconnect-Modul-Einschüben stets auf dieselbe Weise wie die Positionen der Interconnect-Module zugeordnet.

Der Anschluss für die erste Netzwerkschnittstelle auf der Systemplatine eines Blade-Servers wird z. B. immer dem ersten Interconnect-Modul-Einschub eines Gehäuses zugeordnet.

Da das M3-Gehäuse lediglich über vier Interconnect-Modul-Einschübe verfügt, werden zwei Anschlüsse eines Blade-Servers demselben Interconnect-Modul zugeordnet, sofern der Blade-Server komplett mit acht Netzwerkschnittstellen auf drei Netzwerkschnittstellenkarten ausgestattet ist. Die Zuordnung ist nicht durchgängig fortlaufend.

Die folgende Tabelle veranschaulicht die Zuordnung:

Tabelle 5-3 Anschlusszuordnung in einem M3-Gehäuse

Anschluss für Netzwerkschnittstelle	Interconnect-Modul-Einschub
Systemplatine – Anschluss 1	1
Systemplatine – Anschluss 2	1
Tochterkarte 1 – Anschluss 1	2
Tochterkarte 1 – Anschluss 2	2
Tochterkarte 2 – Anschluss 1	3
Tochterkarte 2 – Anschluss 2	4
Tochterkarte 2 – Anschluss 3	3
Tochterkarte 2 – Anschluss 4	4

Im M7-Gehäuse, das acht Interconnect-Modul-Einschübe aufweist, erfolgt die Zuordnung wie in der folgenden Tabelle:

Tabelle 5-4 Anschlusszuordnung in einem M7-Gehäuse

Anschluss für Netzwerkschnittstelle	Interconnect-Modul-Einschub
Systemplatine – Anschluss 1	1
Systemplatine – Anschluss 2	2
Tochterkarte 1 – Anschluss 1	3
Tochterkarte 1 – Anschluss 2	4
Tochterkarte 2 – Anschluss 1	5
Tochterkarte 2 – Anschluss 2	6
Tochterkarte 2 – Anschluss 3	7
Tochterkarte 2 – Anschluss 4	8

Anschlusszuweisungen

In der folgenden Tabelle sind die Anschlüsse aufgeführt, die den Netzwerkschnittstellen in einem G6-Blade-Server-Modell zugewiesen sind. Außerdem sind die Namen der Netzwerkschnittstellen aufgelistet, die vom Betriebssystem verwendet werden.

Die Modelle der Netzwerkschnittstellenkarten sind ebenfalls angegeben.

Tabelle 5-5 Anschlusszuweisungen auf einem G6-Blade-Server

Kartenmodell	Anschluss für Netzwerkschnittstelle	Schnittstellenname des Betriebssystems
HP NC 352i	Systemplatine – Anschluss 1	eth6
	Systemplatine – Anschluss 2	eth7
HP NC 360m	Tochterkarte 1 – Anschluss 1	eth0
	Tochterkarte 1 – Anschluss 2	eth1
HP NC 364m	Tochterkarte 2 – Anschluss 1	eth2
	Tochterkarte 2 – Anschluss 2	eth3
	Tochterkarte 2 – Anschluss 3	eth4
	Tochterkarte 2 – Anschluss 4	eth5

In der folgenden Tabelle sind die Anschlusszuweisungen auf dem G6.5-Blade-Server-Modell aufgeführt.

Tabelle 5-6 Anschlusszuweisungen auf einem G6.5-Blade-Server

Kartenmodell	Anschluss für Netzwerkschnittstelle	Schnittstellenname des Betriebssystems
HP NC 352i	Systemplatine – Anschluss 1	eth6
	Systemplatine – Anschluss 2	eth7
HP NC 382m	Tochterkarte 1 – Anschluss 1	eth4
	Tochterkarte 1 – Anschluss 2	eth5
HP NC 364m	Tochterkarte 2 – Anschluss 1	eth0
	Tochterkarte 2 – Anschluss 2	eth1
	Tochterkarte 2 – Anschluss 3	eth2
	Tochterkarte 2 – Anschluss 4	eth3

In der letzten Tabelle sind die Anschlusszuweisungen auf dem G8-Blade-Server-Modell aufgeführt.

Tabelle 5-7 Anschlusszuweisungen auf einem G8-Blade-Server

Kartenmodell	Anschluss für Netzwerkschnittstelle	Schnittstellenname des Betriebssystems
HP NC 352i	Systemplatine – Anschluss 1	eth0
	Systemplatine – Anschluss 2	eth1
HP NC 360m	Tochterkarte 1 – Anschluss 1	eth2
	Tochterkarte 1 – Anschluss 2	eth3
HP NC 364m	Tochterkarte 2 – Anschluss 1	eth4
	Tochterkarte 2 – Anschluss 2	eth5

Index

A

Active System Console (ASC)
- Allgemein 37
- Installieren 40

Aktivieren des Produkts 18
Ändern der Cache-Volume-Größe 16
Anforderungen
- Physische Appliance 10
- Virtuelle Appliance 10

Anmelden bei der Benutzeroberfläche 18
Anschlusszuweisungen
- Blade-Server 53
- Physische Appliance 23

Appliance
- Aktivieren des Produkts 18
- Anmelden bei der Benutzeroberfläche 18
- Aufspielen eines neuen Images 22
- Durchführen von Upgrades 9
- Einstellungen für serielle Systemkonsolen 23
- Hardware-Verwaltungs-Tools 37
- Physisch 10
- Standardmäßige Erstkonfigurationseinstellungen 11
- Virtuell 10
- Vorinstallierte Software 12

Assistent für das Appliance-Volume 16
Assistenten
- Assistent für das Appliance-Volume 16
- Einrichtungs-Assistent 18
- Konfigurations-Assistent 16

Aufspielen eines neuen Images auf eine Appliance 22

B

Baseboard Management Controller (BMC)
- Allgemein 37
- Konfigurieren 39

Benutzeroberfläche
- Anmeldung 18
- Einrichtungs-Assistent 18

Blade-Server
- Anschlusszuweisungen 53
- Einschalten des Gehäuses 46
- Expliziter Proxy-Modus mit externem Lastausgleich 51
- Gehäuse 43

Blade-Server
- Installieren der Interconnect-Module 45
- Installieren des Blade-Server-Systems 44
- Installieren des Gehäuses 45
- Installieren von Web Gateway anhand eines USB-Laufwerks 48
- Installieren von Web Gateway mit virtuellen Medien 48
- Installieren von Web Gateway über das interne CD/DVD-Laufwerk 47
- Installieren von Web Gateway über ein externes CD/DVD-Laufwerk 48
- Interconnect-Module 45
- McAfee Blade 43
- Proxy, Hochverfügbarkeit 50
- STP (Spanning Tree Protocol) 52
- Transparente Modi 52
- Unterstützte Gehäusemodelle 43
- Unterstütztes Modell 43
- Vorbereiten der Installation eines Blade-Server-Systems 44

D

Datenerfassung
- Konfigurieren 18
- Lesen der Datennutzungserklärung 18

Datennutzungserklärung 18
Dokumentation
- Produktspezifisch, suchen 6
- Typografische Konventionen und Symbole 5

Durchführen eines Upgrades von Web Gateway 9

E

Einrichtung von Web Gateway
- Aktivieren des Produkts 18
- Allgemeine Schritte 9
- Ändern der Cache-Volume-Größe 16
- Anforderungen 10
- Anmelden bei der Benutzeroberfläche 18
- Anschlusszuweisungen 23
- Assistent für das Appliance-Volume 16
- Aufspielen eines neuen Images auf eine Appliance 22
- Beheben von Verbindungsproblemen 21
- Datennutzungserklärung 18
- Einrichtungs-Assistent 18
- Einstellungen für serielle Systemkonsolen 23

Einrichtung von Web Gateway *(Fortsetzung)*
- Einstellungen für virtuelle Maschinen 15
- Erstkonfigurationseinstellungen 16
- Herunterladen der Software für eine physische Appliance 13
- Herunterladen der Software für eine virtuelle Appliance 14
- Herunterladen von Aktualisierungsdateien 18
- Implementieren der standardmäßigen Erstkonfigurationseinstellungen 16
- Implementieren eigener Einstellungen für die Erstkonfiguration 17
- Installieren auf einer physischen Appliance 13
- Installieren auf virtueller Appliance 15
- Konfigurieren der Datenerfassung 18
- Konfigurieren weiterer Ersteinstellungen 20
- Lizenzierung 18
- Physische Appliance mit heruntergeladener Software 12
- Physische Appliance mit vorinstallierter Software 12
- Standardmäßige Erstkonfigurationseinstellungen 11
- Temporärer Lizenzschlüssel 22
- Virtuelle Appliance 14
- Vollständiger Ablauf 18
- Vorinstallierte Software 12

Einrichtungs-Assistent
- Aktivieren des Produkts 18
- Arbeiten mit 18
- Beheben von Verbindungsproblemen 21
- Datennutzungserklärung 18
- Endbenutzer-Lizenzvertrag 18
- Konfigurieren weiterer Ersteinstellungen 20
- Lesen der Online-Dokumente 18
- Öffnen 18
- Vollständiger Einrichtungsablauf 18

Einstellungen
- Eigene Erstkonfiguration 17
- Serielle Systemkonsole 23
- Standardmäßige Erstkonfiguration 11
- Virtuelle Maschine 15
- Weitere Konfiguration 20

Einstellungen für serielle Systemkonsolen 23
Endbenutzer-Lizenzvertrag 18

G

Glasfaser-Netzwerkschnittstellenkarte
- 10GbE-Karte 32
- 1GbE-Karte 30
- Appliance-Modelle 29
- Unterstützte Typen 29

H

Handbuch, Informationen 5
Hardware-Verwaltungs-Tools
- Active System Console (ASC) 37
- Baseboard Management Controller (BMC) 37
- Hardware-Verwaltungs-Tools
- Plattformvertraulichkeitstest (PCT) 37
- Remote Management Module (RMM) 37
- SNMP-Subagent (SNMPSA) 37

K

Konfigurations-Assistent
- Implementieren der standardmäßigen Erstkonfigurationseinstellungen 16
- Implementieren eigener Einstellungen für die Erstkonfiguration 17

Konventionen und Symbole in diesem Handbuch 5

L

Lizenzierung
- Importieren einer Lizenz 18
- Lesen des Endbenutzer-Lizenzvertrags 18
- Temporärer Lizenzschlüssel 22

M

McAfee ServicePortal, Zugriff 6

P

PCI-Karte
- Installieren 34

Plattformvertraulichkeitstest-Tool (PCT)
- Allgemein 37
- Ausführen eines Hardware-Tests 39
- Installieren 38

R

Remote Management Module (RMM)
- Allgemein 37
- Konfigurieren 39

S

ServicePortal, Quellen für Produktinformationen 6
SNMP-Subagent (SNMPSA)
- Aktivieren 41
- Allgemein 37

STP (Spanning Tree Protocol)
- Deaktivieren der Verwendung auf Switches 52
- Zuweisen einer Lastausgleichsrolle 52

T

Technischer Support, Produktdokumentation finden 6

V

Versionshinweise 9